



# SSQ

## STRATEGIC STUDIES QUARTERLY

SPRING 2015

VOL. 9, NO. 1

---

### Commentaries

#### Minuteman for the Joint Fight

Robert L. Butterworth

#### Busting Myths about Nuclear Deterrence

James A. Blackwell Jr.

Charles E. Costanzo

---

### Applying Cost Imposition Strategies against China

Col Kenneth P. Ekman, USAF

---

#### Deterring Malicious Behavior in Cyberspace

Scott Jasper

---

#### Remediating Space Debris: Legal and Technical Barriers

Joshua Tallis

---

#### Power and Predation in Cyberspace

Christopher Whyte

---

#### Fear and Learning in Tehran: What Recent Psychological Research Reveals about Nuclear Crises

Michael D. Cohen

---



## **Chief of Staff, US Air Force**

Gen Mark A. Welsh III

## **Commander, Air Education and Training Command**

Gen Robin Rand

## **Commander and President, Air University**

Lt Gen Steven L. Kwast

## **Director and Publisher, Air Force Research Institute**

Allen G. Peck

### ***Editorial Staff***

Col W. Michael Guillot, USAF, Retired, *Editor*

Ernest A. Rockwell, PhD, *Content Editor*

Vivian D. O'Neal, *Prepress Production Manager*

Tammi K. Dacus, *Editorial Assistant*

Daniel M. Armstrong, *Illustrator*

### ***Advisors***

Gen Michael P. C. Carns, USAF, Retired

Allen G. Peck

Christina Goulter, PhD

Colin S. Gray, DPhil

Robert P. Haffa, PhD

Charlotte Ku, PhD

Benjamin S. Lambeth, PhD

John T. LaSaine, PhD

Allan R. Millett, PhD

Rayford Vaughn, PhD

### ***Contributing Editors***

#### *Air Force Research Institute*

Anthony C. Gould, PhD

#### *School of Advanced Air and Space Studies*

Stephen D. Chiabotti, PhD

James W. Forsyth Jr., PhD

#### *The Spaatz Center*

Charles E. Costanzo, PhD

Christopher M. Hemmer, PhD

Kimberly A. Hudson, PhD

Nori Katagiri, PhD

Paul J. Springer, PhD

Zachary J. Zwald, PhD

*Strategic Studies Quarterly (SSQ)* (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL. Articles in SSQ may be reproduced free of charge. Notify editor and include a standard source credit line on each reprint.



# STRATEGIC STUDIES QUARTERLY

*An Air Force-Sponsored Strategic Forum on  
National and International Security*

VOLUME 9

SPRING 2015

NUMBER 1

## Commentaries

- Minuteman for the Joint Fight* ..... 3  
Robert L. Butterworth
- Busting Myths about Nuclear Deterrence* ..... 17  
James A. Blackwell Jr.  
Charles E. Costanzo

## Feature Article

- Applying Cost Imposition Strategies against China* ..... 26  
Col Kenneth P. Ekman

## Perspectives

- Deterring Malicious Behavior in Cyberspace* ..... 60  
Scott Jasper
- Remediating Space Debris: Legal and Technical Barriers* ..... 86  
Joshua Tallis
- Power and Predation in Cyberspace* ..... 100  
Christopher Whyte
- Fear and Learning in Tehran: What Recent Psychological  
Research Reveals about Nuclear Crises* ..... 119  
Michael D. Cohen

20150310108

## Book Reviews

- Airpower in Afghanistan 2005–10:  
The Air Commander's Perspectives* ..... 139  
By: Dag Henriksen  
Reviewed by: CAPT Jerry L. Gantt, USNR, Retired
- Cybersecurity and Cyberwar:  
What Everyone Needs to Know* ..... 141  
By: P. W. Singer and Allan Friedman  
Reviewed by: Chris Bronk
- Imperial Crossroads:  
The Great Powers and the Persian Gulf* ..... 143  
By: Jeffrey R. Macris and Saul Kelly  
Reviewed by: John Miglietta
- Forging China's Military Might: A New Framework  
for Assessing Innovation* ..... 145  
Edited by: Tai Ming Cheung  
Reviewed by: Lt Col John H. Modinger, PhD, USAF

# Minuteman for the Joint Fight

The United States has been working to modernize its strategic nuclear capabilities, updating warheads through service life extension programs (SLEP) managed by the National Nuclear Security Administration (NNSA) and recapitalizing the Department of Defense's (DOD) legacy triad of delivery systems—bombers, land-based intercontinental ballistic missiles (ICBM), and submarine-launched ballistic missiles (SLBM). Schedules and budgets have been adjusted several times, and plans for the nuclear stockpile of the future now envision only five types of warheads for missiles and bombs.

As yet, the basic triad itself has been unaltered, but even that might come to be questioned, as the budget pressures on plans for maintaining and modernizing the missile and air forces are forecast to be acute. There are no official estimates of the cost of completing all the proposed maintenance and modernization work; unofficial estimates range to \$1 trillion.<sup>1</sup> In any event, it is plain that earlier plans called for too much to be done too quickly. In June 2014 the Navy told Congress that its program to acquire a new submarine force for launching ballistic missiles is financially “unsustainable.”<sup>2</sup> The Senate Armed Services Committee voted out and the House of Representatives passed legislation to create an unprecedented separate “National Sea-Based Deterrence Fund.”<sup>3</sup> Unofficial analyses conclude that the US Air Force (USAF) is facing a similar difficulty and is looking for a similar “national” solution for its plans to modernize both the ICBM and bomber forces, acquire a new long-range standoff cruise missile, and make the F-35 Lightning II stealth multirole fighter capable of delivering nuclear weapons while operating in nuclear environments.<sup>4</sup> The NNSA will be facing similar pressures during the 2020s as it tries to complete the SLEP for the B-61 gravity bomb, begin SLEP work on at least one other missile warhead, develop secure and reliable interoperable warheads for the submarine-launched and land-based long-range ballistic missiles, and reduce the active stockpile to five types of weapons.<sup>5</sup>

The DOD must also keep the currently deployed triad forces in good operating order—an objective that has required repeated special efforts over the past several years. In July 2014 the chief of naval operations warned Congress that ships currently powered by nuclear reactors, including SLBM-carrying submarines, will not be safe unless the FY2015

budget planned for the naval reactors program is increased by \$1.5 billion.<sup>6</sup> A few months later, the 2014 Nuclear Enterprise Review found deficiencies in nuclear force operations and maintenance. As a result, the secretary of defense announced plans to increase funding for the nuclear forces in the defense budget by \$1.5 billion each year for at least the next five years.<sup>7</sup> In addition, the DOD annually sends more than a billion dollars to the NNSA to support work on the warheads for the triad.<sup>8</sup>

Sometimes defense programs need to find ways to do more with less; in this case, it is a question of having more but still not enough, and there are no easy options. In matters of force development, of course, “fiscal pressures” are effectively gauges registering consensus on a program’s anticipated strategic or military importance, and there is no doubt that a safe, secure, survivable, and reliable strategic nuclear force will be essential into the future. The practical effectiveness of that force, the delivery systems, and the warheads they deliver will depend on how well the force suits the challenges of the future strategic environment.

Perhaps that environment will call for capabilities other than version 2.0 of the triad. In particular, the nuclear portfolio could be focused more tightly on two different delivery systems: airplanes and submarine-launched missiles, each of which offers unique capabilities for meeting potential challenges. For several decades the ICBM force provided great capability, but it no longer makes a unique contribution. Today, the submarine force matches or exceeds the ICBM force in lethality, survivability, and responsiveness.<sup>9</sup> Moreover, the ICBMs will no longer provide a completely independent hedge against a surprise technical failure in the sea-launched missiles.<sup>10</sup>

Once removed from their nuclear mission, the ICBMs would still provide an important strategic capability if they were repurposed—a mission change similar to that made with four *Ohio*-class submarines during the early 2000s.<sup>11</sup> All Minuteman III missiles could be refitted with non-nuclear warheads, then providing a unique and valuable capability for responding to a wide range of national security challenges. Quite unlike the “conventional prompt global strike” (CPGS) concepts debated in recent years, conversion of the ICBM force would go well beyond a limited niche capability to provide a strategic strike force useful in fighting wars large and small, as well as enhancing core strategic and extended deterrence postures. The path forward seems likely to prove energizing and free of sharp dislocations to the USAF, the communities surrounding its

missile fields, and American national security policy. Taking that path can also help avoid a repeat of what Gen Maxwell Taylor found in 1959: “The determination of US strategy has become a more or less incidental by-product of the administrative process of the defense budget.”<sup>12</sup>

## Earlier Plans Derailed

The idea of using long-range ballistic missiles as conventional ordnance became popular as the years after the Cold War gave rise to diverse threats around the world.<sup>13</sup> By the end of the 1990s, US military technology was promising a near-term ability to use conventional warheads against some targets that previously had required nuclear weapons. At the turn of the century, a prominent research center called for reducing nuclear expenditures in favor of precision-strike and electronic warfare systems, effectively creating “a new strategic strike triad” of offensive capabilities that would replace the strategic nuclear triad of ICBMs, SLBMs, and bombers.<sup>14</sup> The George W. Bush administration modified this idea for its 2001 Nuclear Posture Review (NPR), which set out to update the dominant strategic planning framework—a Cold War legacy focused primarily on deterring the Soviet Union by means of the nuclear triad. This 2001 NPR portrayed a new strategic environment in which “multiple contingencies and new threats” might arise in several different areas with little warning. To make the US military effective in dissuading, deterring, and defeating these disparate challenges, the NPR advocated a new triad planning framework in which nuclear and nonnuclear strategic strike systems together constituted one apex, with defenses and industrial base capabilities as the other two—all linked by advanced intelligence and communications capabilities.<sup>15</sup>

In 2003 the DOD formally established the requirement for a conventional prompt global strike capability. At that time, the USAF talked about making “global strike” an important capability of the nonnuclear strategic strike component of the new triad—useful for major warfighting and engaging fleeting or emergent targets—although acknowledging that developing an affordable long-range standoff capability was proving difficult.<sup>16</sup> President Bush assigned the operational requirement to US Strategic Command in early 2003, without establishing a single view of what it was to entail, leaving the Air Force, Navy, Army, and Defense Advanced Research Projects Agency to pursue different approaches to



ballistic and partial ballistic delivery systems, reentry systems, and warheads.<sup>17</sup> DOD leaders reportedly hoped to achieve consensus on the mission, associated capabilities, and budgets by 2008, when various studies of organizational interfaces and procedures were to be completed.<sup>18</sup>

The al-Qaeda strikes on 11 September 2001 not only validated NPR's conclusions of 2001, the attacks and subsequent events also transmogrified US perspectives, priorities, and programs. Notwithstanding the broad strategic rationale that was advanced for global strike when the NPR began to be briefed in January 2002, it was probably inevitable that the mission for global strike would be defined by the missed opportunity in December 2001 to kill Osama bin Laden at Tora Bora.<sup>19</sup> Regardless of whether a capability for prompt global strike would have been able to accomplish this task, the effect of the illustration was to narrow the mission, reducing the range of global strike applications. The applications were limited to those particular instances defined by special circumstances in which accurate and reliable intelligence called for an absolutely urgent strike by a system with unprecedented accuracy at intercontinental ranges and for which exact target information was available, when no other option could accomplish the mission.<sup>20</sup> Thus narrowed, the mission appears to be less relevant, which in turn devalues the strategic merit of a CPGS capability and makes it look out of proportion to the cost and risks of using it.<sup>21</sup>

Paramount among those risks, as seen by Congressional leaders and several commentators, are worries that Russia or China might mistakenly identify a long-range missile launch by the United States as a nuclear attack and so trigger a retaliatory nuclear attack. As a result, by 2008 Congress had demanded studies addressing the possibility of "warhead ambiguity," directed that no money be spent on launching conventional warheads by ICBMs or SLBMs, and created a single budget account for prompt global strike research.<sup>22</sup> Congressional budget actions currently continue to deny work on all-ballistic global strike systems, instead favoring delivery systems that would start with a ballistic launch and transition to a hypersonic boost-glide delivery stage. This preference seems likely to reflect opposition to the idea of any CPGS capability, rather than an expectation that Russia or China would be less worried about a system they could not track.<sup>23</sup> The boost-glide systems are far less technologically mature than the ballistic delivery option, and



as of late 2014 it seemed likely another decade or more will be needed before the technology will be ready for program acquisition.

With the mission less compelling and the technology still immature for hypersonic boost-glide systems (currently the only alternatives under development), any prospect for a near-term CPGS capability has vanished.<sup>24</sup>

## **Strategic Strike Redux**

If the United States were to arm all its ICBMs only with conventional weapons, there would be much less about which to worry. The ambiguity problem would not disappear, but its seriousness could be greatly reduced, because the United States simply would not have any nuclear-armed ICBMs deployed, no matter from where they were launched or the trajectory they followed. The record of military responses to potentially escalatory incidents among the United States and Russia and China suggests that history, together with the immediate circumstances of a launch event, will affect the likelihood of its being misinterpreted and the actions that might then be taken: e.g., US-Soviet incidents at sea, a Norwegian missile launch, Russian bombers and fighter aircraft penetrating the air defense identification zone of the United States and Canada, and Chinese fighter aircraft forcing down a US intelligence airplane. As the National Academy concluded, the “significance [of the ambiguity] depends not primarily on the technical characteristics of the CPGS system but on the context, scale, and target of the attack and on the degree to which transparency and confidence-building measures have been employed.”<sup>25</sup> The 2007 Defense Science Board study also found that concerns about ambiguity were overstated.<sup>26</sup>

Whatever worries might remain about warhead ambiguity might be assuaged by public declarations, private notifications, and on-site inspections. Further, a “bolt from the blue” US attack against Russia or China would be most unlikely to use only a few missiles or to launch them on indirect azimuths. Both Russia and China understand strategic intercontinental targeting quite well. Russia is credited with the technical ability to track ballistic missile launches from the United States and, thereby, is able to discriminate between those that are targeted against Russia from those aimed elsewhere.<sup>27</sup> To date, China has taken a different approach, showing no public interest in deploying systems to detect and track launches of foreign long-range missiles. Both these countries

have recently been redeploying strategic forces in ways that increase their survivability, and neither their past behaviors nor strategic cultures support the likelihood that warhead ambiguity would trigger either to launch attacks against the United States.<sup>28</sup> Russian leaders may even start developing their own conventional ICBMs.<sup>29</sup>

An all-conventional ICBM force offers substantial further benefits that go far beyond reducing warhead ambiguity. They provide a significant warfighting capability.<sup>30</sup> Essentially artillery with intercontinental range, the conventional Minuteman force would provide extratheater options for conducting a strategic strike, “a military operation undertaken by the United States that is designed to alter decisively an adversary’s course of action in a relatively compact period of time,” either in isolation or as part of a broader political-military campaign.<sup>31</sup> It could help US forces in regional wars gain access; clear landing zones; destroy launch sites, ports, airfields, and communication centers; penetrate sophisticated air defenses; deny sanctuaries; and kill enemy troop formations. It provides military options for responding to armed aggression when an attack is first underway. It provides additional assurance to allies and partners that the United States can provide timely assistance without being self-deterred. It can ensure dominance under the nuclear threshold, helping control escalation, because no militarily compelling defense against ICBMs is in the offing. It enriches the menu of options available for adaptive planning in crises or even in nuclear warfare.<sup>32</sup> This repurposing of the ICBM force would provide a new means to achieve timely, needed effects on the battlefield, a means that offers economy of force without a lengthy logistics train, that can be used before an adversary has time to prepare defenses or take hostages as a crisis builds, and that, unlike close engagement or stealth options, puts no American lives at risk.

## Enlarging Choices

The future conventional ICBM force could evolve to purpose-built missiles with warheads delivering a variety of effects. When hypersonic technology is sufficiently advanced, the first two stages of the Minuteman missiles could be used to launch new boost-glide payloads that could provide detailed local reconnaissance, extended communications, and persistent surveillance. Their launch and trajectories would be quite

different from entirely ballistic systems—a difference that might relieve them from risks associated with payload ambiguity. However, the hypersonic systems pose a problem of “destination” ambiguity, because the aero vehicle and payload—being maneuverable and very fast—will be difficult to track. The United States might have firsthand experience with the issue, if China’s recent work with hypersonic systems succeeds and Russia pursues similar technology.<sup>33</sup>

Until then, the repurposed Minuteman missiles would be delivering conventional warheads on fully ballistic trajectories, for which better accuracy and new warheads would be useful.<sup>34</sup> The Navy’s earlier work on improving accuracy for the conventional Trident missile might be adaptable to the Minuteman; the National Academy review reported that experiments with the “Enhanced Effectiveness” and “Life Extension” test beds showed promising results, the former in particular suggesting that Global Positioning System–quality accuracy could be achieved for the conventional Trident.<sup>35</sup> Warheads feasible in the near term include designs for kinetic strikes, for penetrating hard surfaces, and, for above-ground soft targets, the kinetic energy projectile, which promises to deliver thousands of tungsten flechettes to clear an area of 3,000 square feet—roughly a radius of 10 yards.<sup>36</sup> Of course, the likelihood of killing the target can also be increased by launching more than one missile.

Uncertainty about the emerging strategic environment, particularly about Russian and Chinese nuclear postures, makes it prudent to retain for a while the ability to reverse course and make the Minuteman once again a nuclear weapon system, at least until the use of conventional long-range ballistic missiles becomes commonplace and future requirements for strategic nuclear weapons become more settled. Because international relations would have severely deteriorated before the United States would consider rearming the missiles with nuclear warheads and because doing so probably could not be accomplished very quickly or secretly, it is unlikely any warhead ambiguity problem would be exacerbated by keeping the Minuteman capable of launching both types of warheads. Shorter-range “dual-capable” delivery systems have been deployed elsewhere by the United States and other countries. Once converted to conventional warheads, then, the Minuteman missiles could stay in the same silos they used before the nuclear warheads were removed, until the United States determined that a rearming hedge was no longer necessary. However, plans for using the conventionally armed



missiles from their current silos will need to take into account potential hazards from the falling canopies and stages jettisoned during the first minutes of flight; perhaps silos, not nuclear-hardened, could be built for coastal launching.<sup>37</sup>

Even with the nuclear warheads removed, the Minuteman force would still be counted against the total number of operationally deployed launchers and warheads allowed under the New Strategic Arms Reduction Treaty (START). Operationally deployed US nuclear warheads would thus be reduced by 400—26 percent below the allowed total of 1,550. The effect of this unilateral reduction on US nuclear deterrence deserves careful review, but any perceived risks would be mitigated somewhat by maintaining the missiles in their silos and by maintaining the ability to restore their nuclear warheads. The reduction may in fact never occur, because the New START could be modified in 2021.<sup>38</sup> If the United States has made good progress in conversion by then, US negotiators might want to exempt the Minuteman force from strategic nuclear force limits, particularly if Russia and China have made progress developing similar capabilities. If the same aggregate limits were maintained, the United States could then choose to deploy 400 nuclear warheads with additional strategic bombers or SLBMs.

The effect on US deterrence of moving from three to two strategic nuclear delivery systems is a question separate from the reduction in numbers. The advantages of the ICBMs over the SLBMs in earlier decades (promptness, accuracy, throw-weight) no longer apply. Removing the ICBM nuclear warheads would not make an enemy's defense problems easier; the diversity of attack azimuths and trajectories offered by the sea-based force actually creates a more complicated issue. Nor would an enemy attack plan be simpler. In the event of nuclear war, an enemy will still want to target the land-based missiles, even the conventional ones.<sup>39</sup>

Making the Minuteman force a conventional capability would relieve some pressure on budgeting for the strategic nuclear forces. The NNSA would no longer need to develop an interoperable warhead, and the DOD nuclear budget would no longer need the level of funding required previously for operations and maintenance—especially physical and personnel security—and for modernization. The nonnuclear budgets would see increased costs, estimates for which will depend on plans for developing needed subsystems (particularly the conventional warheads), decisions about whether and how to maintain a renucleariza-

tion hedge, warhead replacement and storage, training, command and control systems, and so forth. The estimated net costs, whatever they turn out to be, must then be assessed in light of the military utility of the repurposed missiles to conventional force planning and operations and to joint force development aimed at defeating anti-access and area denial efforts by potential adversaries.

## Conclusion

As the Defense Science Board reported in 2003, “Strategic strike, then, is more than just taking a shot at a target.”<sup>40</sup> The repurposed Minuteman missiles would be an integral part of the joint fight, woven into the ongoing development of strategy, plans, and exercises and tailored to suit particular circumstances when needed. Circumstances permitting, these missiles could execute many of the particular missions identified as appropriate in discussions of CPGS capabilities. But the repurposed Minuteman force would not be confined to residual niche assignments. Instead, the new force would contribute directly and substantially to three of the current administration’s “five key objectives” for nuclear weapons: “reducing the role of U.S. nuclear weapons in U.S. national security strategy; maintaining strategic deterrence and stability at reduced nuclear force levels; and strengthening regional deterrence and reassuring U.S. allies and partners.”<sup>41</sup> Most important, it will provide options that a US president does not now have for managing crises and resisting aggression. ■■■

**Robert L. Butterworth**

*President, Aries Analytics, Inc.*

*A Virginia-based national security consultancy*

## Notes

1. Jon B. Wolfsthal, Jeffrey Lewis, and Marc Quint, *The Trillion Dollar Nuclear Triad: US Strategic Nuclear Modernization over the Next Thirty Years* (Monterey, CA: James Martin Center for Nonproliferation Studies, January 2014), [http://cns.miis.edu/opapers/pdfs/140107\\_trillion\\_dollar\\_nuclear\\_triad.pdf](http://cns.miis.edu/opapers/pdfs/140107_trillion_dollar_nuclear_triad.pdf).

2. The planned force “requires funding at an unsustainable level, particularly between FY25 and FY34. . . . The average cost of this plan during the period in which the [Department of Navy] is procuring the [*Ohio*-class replacement SLBM-launching submarine] (~\$19.7 B/year FY2015–2034) cannot be accommodated by the Navy from existing resources—particularly

if DOD is required to be funded at the [Budget Control Act] levels.” Deputy Chief of Naval Operations, *Report to Congress on the Annual Long-Range Plan for Construction of Naval Vessels for FY2015* (Washington, DC: Office of the Chief of Naval Operations, June 2014), 6, <http://navylive.dodlive.mil/files/2014/07/30-year-shipbuilding-plan1.pdf>.

3. National Journal, “Navy: Plan to Build New Strategic Sub Requires ‘Unsustainable’ Funding,” *Global Security Newswire*, 8 July 2014, <http://www.nti.org/gsn/article/us-navy-says-plan-build-new-strategic-sub-requires-unsustainable-funding/>.

4. See Kingston Reif, “The Air Force Can’t Hide from the Cost of Nuclear Weapons,” *Center for Arms Control and Non-Proliferation* (web site), 21 August 2014, [http://armscontrolcenter.org/issues/nuclearweapons/articles/the\\_air\\_force\\_cant\\_hide\\_from\\_the\\_cost\\_of\\_nuclear\\_weapons/](http://armscontrolcenter.org/issues/nuclearweapons/articles/the_air_force_cant_hide_from_the_cost_of_nuclear_weapons/).

5. See Government Accountability Office, *Modernizing the Nuclear Security Infrastructure: NNSA’s Budget Estimates Do Not Fully Align with Plans*, GAO-14-45 (Washington, DC: General Accountability Office, December 2013), <http://www.gao.gov/assets/660/659610.pdf>.

6. Christopher P. Cavas, “US Navy to Congress: We Can’t Guarantee a Safe Nuclear Fleet,” *Defense News*, 9 July 2014, <http://www.defensenews.com/article/20140709/CONGRESS-WATCH/307090028/US-Navy-Congress-We-Can-t-Guarantee-Safe-Nuclear-Fleet>.

7. See Chuck Hagel, secretary of defense, “Reforms to the Nuclear Enterprise,” press conference, transcript, 14 November 2014, <http://www.defense.gov/Transcripts/Transcript.aspx?TranscriptID=5537>. Earlier problems with management of the nuclear forces, particularly by the USAF, had occasioned several reviews, including the “Air Force Blue Ribbon Review on Nuclear Weapons Policies and Procedures” (February 2008); the secretary of defense–directed “Investigation in the Shipment of Sensitive Missile Components to Taiwan” (May 2008); the “Secretary of Defense Task Force on Nuclear Weapons Management” (September 2008); a report by the Defense Science Board’s Permanent Task Force on Nuclear Weapons Surety, “Report on the Unauthorized Movement of Nuclear Weapons” (February 2008); testimony by Maj Gen C. Donald Alston to the Strategic Forces Subcommittee of the House Armed Services Committee, “Status of the Air Force Nuclear Security Roadmap” (21 January 2010); and two further reports from the Defense Science Board’s Permanent Task Force: the final “Independent Assessment of the Air Force Nuclear Enterprise” (April 2011), and the subsequent final “Air Force Nuclear Enterprise Follow-on Review” (May 2013).

8. Department of Energy, *FY2014 Congressional Budget Request: National Nuclear Security Administration*, vol. 1 (Washington, DC: DOE, April 2013), WA-5, note a, [http://fire.pppl.gov/FY14\\_Budget\\_NNSA\\_details.pdf](http://fire.pppl.gov/FY14_Budget_NNSA_details.pdf).

9. General Accountability Office “Unclassified Summary Statement on the GAO Triad Project,” PEMD-92-36R Triad Summary (Washington, DC: GAO, 28 September 1992), 5, <http://gao.gov/assets/90/82669.pdf>. “On balance, the sea leg emerges as the most cost-effective, taking into account [seven measures of effectiveness]. Test and operational patrol data show that the speed and reliability of day-to-day communications to submerged, deployed SSBNs [submarines equipped to launch long-range strategic missiles] were far better than widely believed, and about the equal of speed and reliability of communications to ICBM silos. Contrary to conventional wisdom, SSBNs are in essentially constant communication with National Command Authorities and, depending on the scenario, SLBMs would be almost as prompt as ICBMs in hitting enemy targets.”

10. Commonality is often seen as a means to sustain the missile industrial base and thereby reduce future costs of modernization. In 2007, for example, Senators Orrin Hatch and Bob Bennett introduced legislation with a provision directing the secretary of defense to provide “an analysis of the impact on materials, the supplier base, production facilities, and



the production workforce of extending all or part of the service life extension program for the Trident II D5 missile system to a service life extension program for the Minuteman III intercontinental ballistic missile system.” *Strategic Deterrent Sustainment Act of 2007*, S. 2039, 110th Cong., 1st sess., *Congressional Record* 153, no. 134 (11 September 2007): S11416–S11418. Four years later, Rear Adm Terry Benedict, head of the Navy’s strategic systems programs, told a Navy conference that “We currently have collaboration efforts with the Air Force . . . [which might include a] common fuse for the Minuteman’s W78 warhead and the Trident’s W88; common guidance systems R&D, common propulsion R&D; electronic systems; ordnance; and tooling.” Philip Ewing, “A Joint Navy-Air Force Ballistic Missile?” *DoD Buzz*, 21 October 2011, <http://www.dodbuzz.com/2011/10/21/a-joint-navy-air-force-ballistic-missile/>. A year later Admiral Benedict was reported as saying that the Navy and USAF would be collaborating on research and development and components that could be used by both services, such as gyroscopes and rocket-fuel constituents, and that “the future is going to be much more intertwined between these two services. Collaboration and commonality is not an option, it is a requirement.” Sydney J. Freeberg Jr., “Navy Fears Pentagon Neglects New Missile Sub; SSBN(X) Must Survive Almost 80 Years,” *Breaking Defense*, 18 October 2012, <http://breakingdefense.com/2012/10/navy-fears-pentagon-neglects-new-missile-sub-ssbn-x-must-survi/>.

11. David Nagle, “SSGN Provides Powerful Tool for Navy SEALs,” *Navy News Service*, 7 February 2003, [http://www.navy.mil/submit/display.asp?story\\_id=5767](http://www.navy.mil/submit/display.asp?story_id=5767).

12. Maxwell D. Taylor, *The Uncertain Trumpet* (New York: Harper & Brothers, 1959), 121.

13. National Defense Panel, *Transforming Defense: National Security in the 21st Century* (Washington, DC: DOD, December 1997), [http://www.dod.gov/pubs/foi/administration\\_and\\_Management/other/902.pdf](http://www.dod.gov/pubs/foi/administration_and_Management/other/902.pdf).

14. “A strong case can be made that the United States should take steps to create a new strategic-strike triad, relying on its precision- and electronic-strike capabilities to form two of the three legs, with a smaller residual nuclear force comprising the third leg.” Andrew F. Krepinevich Jr. and Robert C. Martinage, *The Transformation of Strategic-Strike Operations* (Washington, DC: Center for Strategic and Budgetary Alternatives, 2001), i, <http://www.csbaonline.org/wp-content/uploads/2011/03/2001.03.01-Strategic-Strike-Operations.pdf>.

15. See Amy Woolf, *The Nuclear Posture Review: Overview and Emerging Issues* (Washington, DC: Congressional Research Service, 31 January 2002), <http://fpc.state.gov/documents/organization/8039.pdf>; and Kurt Guthe, *How is the “New Triad” New?* (Washington, DC: Center for Strategic and Budgetary Alternatives, 29 July 2002), <http://www.csbaonline.org/wp-content/uploads/2011/03/2002.07.29-Nuclear-Posture-Review-The-New-Triad.pdf>.

16. *US Air Force Transformation Flight Plan* (Washington, DC: Headquarters, US Air Force, XPXC, November 2003), [http://www.au.af.mil/au/awc/awcgate/af/af\\_trans\\_flightplan\\_nov03.pdf](http://www.au.af.mil/au/awc/awcgate/af/af_trans_flightplan_nov03.pdf). For example, “The Global Strike CONOPS is designed, among other tasks, to defeat air defense systems,” C-7; and “At the start of conflict, Global Strike capabilities will “kick down the door” into denied battlespace by rapidly degrading, and then defeating, the adversary’s battle-space awareness and anti-access capabilities, clearing the way for joint persistent follow-on operations,” 44. “Potential adversaries have become increasingly hesitant to oppose the US military force-on-force and are seeking new ways to counter American strengths. Instead, they are dispersing their critical systems into sensitive areas with high collateral damage potential, in deeply buried bunkers or tunnels, and employing asymmetric offensive capabilities such as terrorist acts, network attack, or subversive media campaigns that undermine coalitions and sway international opinion. Consequently, some US targets have changed from fixed, fielded forces to a series of fleeting and emergent targets.” 43. “Reducing the cost of the

weapons while maintaining long-range has proven very difficult. . . . Developing an affordable standoff weapon that would enable large scale, persistent standoff operations against fixed and mobile targets in all weather would create a huge transformational effect in defeating future advanced air defenses. Standoff will also be a key enabler of the Joint Commander's ability to use the Global Strike CONOPS' capabilities to operate successfully in heavily defended airspace at the start of a conflict and the Global Response CONOPS' capabilities to conduct rapid response operations against terrorist-related targets." 59.

17. See the discussion in Vince Manzo, *An Examination of the Pentagon's Prompt Global Strike Program: Rationale, Implementation, and Risks* (Washington, DC: Center for Defense Information 2008), [http://www.infodefensa.com/wp-content/uploads/PGSfactsheet\[1\].pdf](http://www.infodefensa.com/wp-content/uploads/PGSfactsheet[1].pdf); and the report by the General Accountability Office, *Military Transformation: DOD Needs to Strengthen Implementation of its Global Strike Concept and Provide a Comprehensive Investment Approach for Acquiring Needed Capabilities* (Washington, DC: General Accountability Office, GAO-08-325, 30 April 2008), <http://www.gao.gov/assets/280/274988.pdf>.

18. GAO, *Military Transformation*, 10–11.

19. The bin Laden case is used to illustrate the mission for the Prompt Global Strike weapon as described in David E. Sanger and Thom Shanker, "U.S. Faces Choice on New Weapons for Fast Strikes," *New York Times*, 22 April 2010, [http://www.nytimes.com/2010/04/23/world/europe/23strike.html?\\_r=0](http://www.nytimes.com/2010/04/23/world/europe/23strike.html?_r=0).

20. Critics narrowed the mission and then challenged its feasibility. For example, "The US agencies involved in counterterrorism should attempt to identify historical examples of occasions when the United States has failed to capitalize on intelligence that would have enabled it to kill or capture an important terrorist because it lacked a CPGS capability. Former senior officials could be brought in to judge whether the available intelligence would actually have been persuasive enough to prompt a president to use a CPGS weapon, had one been available." James M. Acton, *Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike* (Washington, DC: Carnegie Endowment for International Peace, 2013), 94, <http://carnegieendowment.org/files/cpgs.pdf>.

21. Some critics also stress potential complexities, delays, and costs in the CPGS "enabling" functions, noting that a target should be acquired before the weapon is launched, which can be difficult if the target is moving; that authorization and delegation procedures will be needed, together with reliable communications; and that intelligence might be mistaken. Steve Andreasen provided an early catalogue of concerns in his "Off Target? The Bush Administration's Plan to Arm Long-Range Ballistic Missiles with Conventional Warheads," *Arms Control Association* (web site), 8 July 2006, [http://www.armscontrol.org/act/2006\\_07-08/CoverStory](http://www.armscontrol.org/act/2006_07-08/CoverStory); and Joshua Pollack considered intelligence and delegation problems in his "Evaluating Conventional Prompt Global Strike," *Bulletin of the Atomic Scientists* 65, no. 1 (January 2009): 13–20.

22. See the excellent summary in Amy Woolf, *Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues* (Washington, DC: Congressional Research Service, 26 August 2014), <http://fpc.state.gov/documents/organization/231285.pdf>. Acton claims that the congressional actions were "ostensibly because of warhead ambiguity." Acton, *Silver Bullet?*, 2.

23. See the comparison of warhead and destination ambiguities associated with ballistic and hypervelocity delivery systems in Elaine Bunn and Vince Manzo, *Conventional Prompt Global Strike: Strategic Asset or Unusable Liability?*, *Strategic Forum* 263 (February 2011): 14–18, [http://csis.org/files/media/isis/pubs/110201\\_manzo\\_sf\\_263.pdf](http://csis.org/files/media/isis/pubs/110201_manzo_sf_263.pdf).

24. News reports say that DOD-imposed funding restrictions on the proposed development of a medium-range ballistic missile to be launched from *Virginia*-class submarines, a program denied funding for FY2014 by Senate appropriators, and that “the Pentagon’s Joint Requirements Oversight Council . . . [in November 2012] determined in closed-door session that future technologies for prompt strike must do a better job of balancing affordability with desired warfighting capabilities.” Elaine M. Grossman, “Pentagon, Lawmakers Deal Blows to Navy Fast-Strike Missile Effort,” *Global Security Newswire*, 31 July 2013, <http://www.nti.org/ghn/article/pentagon-lawmakers-deal-blows-navy-fast-strike-missile-effort/>.

25. National Research Council, *U.S. Conventional Prompt Global Strike: Issues for 2008 and Beyond* (Washington, DC: National Academy of Science, 2008), 71–77, [http://www.nap.edu/openbook.php?record\\_id=12061](http://www.nap.edu/openbook.php?record_id=12061).

26. The 2007 Defense Science Board study noted that only peer competitors have the capability to detect and track US launches, concluding that “because of the mutual assured destruction concerns of a major nuclear exchange, peer competitors may be less likely to over-react to a single ballistic missile until they are able to reliably determine its true destination.” Defense Science Board, *Time Critical Strike from Strategic Standoff* (Washington, DC: Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, March 2009; information gathering completed in April 2007).

27. Tatyana Rusakova, “Russia to Upgrade Missile Attack Warning System,” *Russia Beyond the Headlines*, 4 July 2014, [http://rbth.com/defence/2014/07/04/russia\\_to\\_upgrade\\_missile\\_attack\\_warning\\_system\\_37961.html](http://rbth.com/defence/2014/07/04/russia_to_upgrade_missile_attack_warning_system_37961.html).

28. See Robert L. Butterworth, “Out of Balance: Will Conventional ICBMs Destroy Deterrence?” *Aerospace Power Journal* 15, no. 3 (Fall 2001): 74–84, <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj01/fal01/butterworth.html>; Lora Saalman, *Prompt Global Strike: China and the Spear* (Honolulu, HI: Asia-Pacific Center for Security Studies, April 2014), [http://www.apcss.org/wp-content/uploads/2014/04/APCSS\\_Saalman\\_PGS\\_China\\_Apr2014.pdf](http://www.apcss.org/wp-content/uploads/2014/04/APCSS_Saalman_PGS_China_Apr2014.pdf); and Thomas Scheber, “Conventionally-Armed ICBMs: Time for Another Look,” *Comparative Strategy* 27, no. 4 (October 2008): 336–44. On page 343, Scheber describes a senior retired Russian military officer in December 2007 dismissing “as nonsense concerns that Russian officials would misinterpret the launch of a few CPGS weapons and respond with a nuclear strike.”

29. Associated Press, “Russia Developing New Nuclear Weapons to Counter US, NATO,” *New York Post*, 10 September 2014, <http://nypost.com/2014/09/10/russia-developing-new-nuclear-weapons-to-counter-us-nato/>; and “‘Deterrence Not Arms Race’: Russia Hints It May Develop Rival to US Prompt Global Strike,” *RT News*, 11 September 2014, <http://rt.com/news/187092-russia-prompt-global-strike/>.

30. This formulation is broader than one focused on CPGS, but it has much in common with Bruce Sugden’s examples of “the long-term, expanded mission.” Bruce M. Sugden, “Speed Kills: Analyzing the Deployment of Conventional Ballistic Missiles,” *International Security* 34, no. 1 (Summer 2009): 113–46; see especially his discussion on pages 118–21. Guthe notes that conventional strike increases the flexibility of response and discusses sample applications, *How is the “New Triad” New?*, 8–10.

31. *Report of the Defense Science Board Task Force on Future Strategic Strike Forces* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, February 2004), 2-1. Strategic strike “forces include traditional longer-range missile and air assets, missile assets at sea, in-theater air and naval assets, and in-theater special operations forces. Newer information operations capabilities could also be used as part of a strategic strike mission,” 2-2.



32. Barry Watts notes what would be forgone if effective long-range strike capabilities are not developed: "A crucial challenge likely to be unmet is neglecting to hedge against the rise of Asian powers and the spread of nuclear weapons. Other lost opportunities and unmet challenges include: reducing American reliance on nuclear weapons, denying prospective enemies sanctuaries, shaping their investments by forcing them to spend more on defending against American LRS capabilities, and closing capability gaps—preeminently the ability to prosecute emergent and time-sensitive targets deep inside defended airspace. These issues provide the strategic rationale for moving ahead promptly in LRS and are the focus of the second chapter of this report." Barry D. Watts, *Long-Range Strike: Imperatives, Urgency, and Options* (Washington, DC: Center for Strategic and Budgetary Assessments, April 2005), ii.

33. Valerie Insinna, "US, China in Race to Develop Hypersonic Weapons," *National Defense Magazine*, 17 August 2014, <http://www.nationaldefensemagazine.org/blog/Lists/Posts/Post.aspx?ID=1585>; and Kenneth Rapoza, "Like U.S., Latest Russian Bombers Testing Hypersonic Weapons," *Forbes*, 1 September 2013, <http://www.forbes.com/sites/kenrapoza/2013/09/01/like-u-s-latest-russian-bombers-testing-hypersonic-weapons/>.

34. The accuracy required depends generally on the effect required, the warhead lethality, and the target vulnerability. The National Research Council study called for "accuracy on the order of meters" for the Conventional Trident Missile system as sketched in 2008 (*US Conventional Prompt Global Strike*, 14). The 2003 Defense Science Board Summer Study projected a need for CEPs of less than ten meters and called for developing a new conventional intermediate-range ballistic missile with a CEP of less than five meters (*Report of the Defense Science Board Task Force on Future Strategic Strike Forces*, 2–16).

35. National Research Council, *US Conventional Prompt Global Strike*, 121–23.

36. *Ibid.*, 127–131.

37. Potential damage from falling boosters has been taken sometimes as a cost of war (i.e., ground-based interceptor launches from Alaska, ICBM launches against Russia, and Pershing II launches against the Soviet Union) and sometimes as requiring special consideration for public safety (i.e., conventional ICBM launches in limited wars and missile defense launches in Europe).

38. New START entered into force in February 2011 for a term of 10 years, after which it can be extended for an additional five years if the parties agree to do so. Arms Control Association, "New START at a Glance" (factsheet, Arms Control Association, Washington, DC, August 2012), <http://www.armscontrol.org/factsheets/NewSTART>.

39. "Any system—old or new—that the United States might designate as conventional-only . . . could be armed with nuclear weapons. Other countries could never be confident that there is not a nuclear warhead on a new US system simply because the US says so." National Research Council, *US Conventional Prompt Global Strike*, 73.

40. *Report of the Defense Science Board Task Force on Future Strategic Strike Forces*, 2–15.

41. DOD, *Nuclear Posture Review Report* (Washington, DC: DOD, April 2010), iii, <http://www.defense.gov/npr/docs/2010%20Nuclear%20Posture%20Review%20Report.pdf>.

# Busting Myths about Nuclear Deterrence

America is embarked on a quest for a world without nuclear weapons, but we live in a world not yet safe from war and threats of war. Hence, as long as nuclear weapons exist, the United States must maintain a safe, secure, and effective arsenal—both to deter potential adversaries and to assure US allies and other security partners that they can count on US security commitments. Our nuclear posture communicates to potential nuclear-armed adversaries that they cannot use nuclear threats to intimidate the United States, its allies, or partners or escalate their way out of failed conventional aggression. The United States Air Force (USAF) will continue to maintain its responsibilities as steward of two of the nation's three legs of the strategic nuclear triad and the nation's associated nuclear command, control, and communications infrastructure.

Since the Cold War, three states (India, Pakistan, and North Korea) have developed nuclear-weapon capabilities, while Iran remains on course to do so. Moreover, ongoing nuclear modernization programs in China and Russia point to the continued importance of nuclear deterrence and assurance for our allies and partners. Some countries now have military doctrines that include potential first use of nuclear weapons in a militarized crisis, and these countries regularly exercise those doctrines. These threats require the United States to seriously consider its responsibility to educate and advocate for the commitment and investment needed to sustain nuclear deterrence capabilities in a dangerous world.

The commitment must resemble Voltaire's *Candide*, dealing with the world as it is, rather than succumbing to the quest of Cervantes's *Don Quixote*, tilting fatefully at windmills. Currently, there are too many erroneous popular myths accepted uncritically by too many people about US nuclear capability. This commentary serves as a myth buster to elucidate these beliefs and confront them with the facts about America's nuclear arsenal and the purpose that arsenal serves.

## **Myth #1: The United States Does Not Use Nuclear Weapons**

Although no nation has detonated a nuclear weapon in war since 9 August 1945, every US president since Harry Truman has used nuclear weapons to deter or compel adversaries by communicating the message

that the United States is fully capable of employing nuclear weapons under circumstances determined by the National Command Authorities. US Navy ballistic missile submarines (SSBN) and USAF intercontinental ballistic missiles (ICBM) are used 24/7 to deter any nuclear-armed country with hostile intentions against the United States. Moreover, USAF nuclear-capable bombers also have been used to convey national resolve to adversaries and allies.

This was the case with Pres. Barack Obama's decision to fly B-52 and B-2 bombers over the Korean peninsula in March 2013. North Korea had just completed its third nuclear weapons test and successfully launched a space-launch vehicle that clearly showed Kim Jung Un's intent to develop ballistic missiles capable of delivering a nuclear warhead against an Asian ally and possibly US territory. When the global news media noticed a B-2 over Seoul, one international news agency did not report that the bat-winged, radar-evading aircraft had flown a regularly scheduled peacetime exercise. Instead, the outlet stated that the "United States flew two nuclear-capable stealth bombers on practice runs over South Korea . . . in a rare show of force following a series of North Korean threats that the Pentagon said have set Pyongyang on a dangerous path."<sup>1</sup> Chinese, North and South Korean, Russian, European, and US news outlets likewise focused almost exclusively on the nuclear capability of the bombers used in this mission.

Any nuclear-armed state contemplating aggression against the United States recognizes the overwhelming odds against its success and the jeopardy it faces for foolhardy acts. Silo-based ICBMs deployed across America's heartland, SSBNs patrolling beneath the world's oceans, and our nuclear-capable bombers are constant, tangible reminders of the price for nuclear aggression against the United States. *Myth #1 Busted—The fact is the United States uses its nuclear weapons every day.*

## **Myth #2: Nuclear Weapons Have Only Limited Utility for Their Cost**

The USAF spends about \$5 billion a year to maintain ICBMs and bombers to deter nuclear attacks against the United States, and the service is committed to a 10-year, \$83.9 billion strategic modernization plan for its portion of the nation's nuclear deterrent. The Congressional Budget Office reports that the federal government will spend \$355 bil-



lion over the next 10 years for all nuclear weapons investments, including those of the USAF, the Navy, the Department of Defense (DOD), and the Department of Energy.<sup>2</sup> These actual and projected expenditures are by no means insignificant, yet the cost of a weapon system is meaningful only in relation to the capability it provides and the broader purpose it serves. Stated differently, one must measure the merits of a weapon beyond just its monetary cost relative to the threat it confronts.

By deterring the only existential threat that can destroy the United States, nuclear weapons are a bargain. This does not diminish the warfighting capability of conventional forces, but history has shown repeatedly that conventional weapons are not an effective deterrent against major interstate war, and certainly would not be in a nuclear-armed world. In the past, civilian and military leaders often failed to anticipate the costly consequences of war. One need only consider the millions killed in the two world wars of the twentieth century to conclude that conventional forces alone do not deter national leaders determined to undertake large-scale aggression.

Yet, foreign leaders today could hardly fail to grasp the consequences of such aggression against the United States. Carl von Clausewitz observed in his classic work, *On War*, that when the potential exists for extreme violence, states should not take the first step toward war without carefully considering the last step. Because the US nuclear arsenal clarifies and sharpens nuclear-armed adversaries' thinking about war in ways other weapons cannot, those states are wary of taking the first step—because they readily grasp the image of the last step. Nuclear deterrence is thus a bargain against extreme forms of aggression. *Myth #2 Busted—Nuclear weapons are a priceless deterrent until nuclear weapons are verifiably eliminated from all countries' arsenals.*

### **Myth #3: Nuclear Weapons Are Going Away**

Why bother spending billions of dollars to modernize US nuclear forces? Faith in the eventuality of a world devoid of nuclear weapons is the clarion call of the arms control community for radically reduced spending on nuclear weapons.<sup>3</sup> The hope for nuclear disarmament has inspired many US presidents, most recently President Obama, but the twenty-first century presents an incontestable reality of nuclear-armed states, most notably China and Russia.<sup>4</sup> The Congressional Commission

on the Strategic Posture of the United States acknowledged this reality: “The conditions that might make possible the global elimination of nuclear weapons are not present today and their creation would require a fundamental transformation of the world political order.”<sup>5</sup>

The commission observed—with specific reference to uncertainty about China and Russia—that “the U.S. nuclear posture must be designed . . . not just [for] deterrence of enemies in time of crisis and war but also assurance of our allies and dissuasion of potential adversaries. . . . The triad of strategic nuclear delivery systems should be maintained for the immediate future and this will require some difficult investment choices.”<sup>6</sup> In 2014, nearly five years after the commission’s final report was released, the commander of US Strategic Command affirmed that foreign “nuclear powers are investing in long-term and wide-ranging military modernization programs.”<sup>7</sup> Notable among these programs are China’s and Russia’s growing nuclear capabilities.

China’s once modest nuclear force is rapidly evolving in size and in quality. “Over the next three to five years, China’s nuclear program will become more lethal and survivable with the fielding of additional road-mobile nuclear missiles; five nuclear-powered ballistic missile submarines, each carrying 12 sea-launched intercontinental-range ballistic missiles; and ICBMs armed with multiple independently targetable re-entry vehicles.”<sup>8</sup> In late 2014 Beijing tested its first ICBM capable of carrying up to 10 warheads, a development that has been characterized as “a significant advance for China’s strategic nuclear forces and part of a build-up that is likely to affect the strategic balance of forces.”<sup>9</sup> Even the less-favored air-breathing leg of China’s nuclear arsenal will benefit from the addition of the new H-6K bomber, which is equipped with long-range, nuclear-capable Changjian-10 cruise missiles, effectively increasing the aircraft’s combat radius to reach Okinawa, Guam, and Hawaii from the mainland.<sup>10</sup> Russia also continues a robust nuclear modernization program that includes silo-based and mobile versions of the RS-24 and mobile RS-26 ICBMs, both carrying multiple independently targetable reentry vehicles; deployment of up to eight new Borei-class SSBNs, fitted with 16 launch tubes for new Bulava ICBMs (each carrying up to 10 independently targetable warheads); and development of a new long-range bomber to be outfitted with hypersonic missiles.<sup>11</sup> Given the reality of nuclear-armed states and nuclear-weapon aspirants, the United States must make the difficult choices to sustain our nuclear deterrent. *Myth*

*#3 Busted—Nuclear weapons are not going away; rather nuclear states are modernizing their arsenals, while other states seek these weapons.*

### **Myth #4: The United States Can Deter with Submarines Alone**

This myth is predicated primarily on the notion SSBN survivability is “easier to achieve” relative to fixed-site ICBMs and long-range bombers that may be vulnerable on the ground and in the air.<sup>12</sup> However, there are two risks with the submarine-only deterrent myth. First, while some argue the stealth of SSBNs ensures their survival for second-strike missions, the current US chief of naval operations has noted the limits of stealth-based platforms. Adm Jonathan W. Greenert has observed that the “rapid expansion of computing power also ushers in new sensors and methods that will make stealth and its advantages increasingly difficult to maintain above and below the water.”<sup>13</sup> While adversaries probably could not achieve antisubmarine warfare (ASW) breakthroughs in the near term to threaten SSBNs, by divesting itself of the deterrent triad for a SSBN-based monad, the United States would necessarily create a high payoff incentive for adversaries to seek ASW capabilities to neutralize US ballistic missile submarines. Rather than saving defense resources by scrapping ICBM and bomber forces, a new and potentially destabilizing arms race could occur as each side postures and repostures below the world’s oceans.

The second risk of a submarine-only nuclear force is that the United States would have no way to demonstrate intent to nuclear-armed regional adversaries or to allies who rely on US extended deterrence to preserve peace. Locational uncertainty is necessary for SSBNs to preserve their second-strike capability; thus, submariners are highly averse to revealing their position. This vulnerability surrenders their primary method for survivability.<sup>14</sup> However, being visible is exactly what is needed to demonstrate resolve—thus, the reason nuclear-capable bombers are so important. Ballistic missile submarines simply could not do what the B-2 bombers did over Korea in 2013. As the Commission on the Strategic Posture of the United States observed, “each leg of the triad has its own value.”<sup>15</sup> The commission further pointed out that the unique and synergistic characteristics of the triad will remain “valuable as the number of operationally deployed strategic nuclear weapons” de-

clines.<sup>16</sup> *Myth #4 Busted—The United States cannot safely deter nuclear aggression with a SSBN-based monad alone.*

### **Myth #5: The USAF Is Stuck in a Cold War Mind-Set**

Although the United States took an intellectual holiday from thinking about nuclear deterrence following the Cold War, the USAF has undertaken a fundamental transformation of its approach to thinking about nuclear weapons in the twenty-first century.<sup>17</sup> Secretary of the Air Force Deborah James has noted the diminished understanding of deterrence across the nuclear enterprise and within the USAF, even among senior leaders, and she has made a forceful call for USAF professionals to reestablish their intellectual leadership on deterrence. In addition to dozens of immediate actions under its Force Improvement Programs, the USAF is undertaking longer-range reform of its doctrine, professional military education (PME) for all Airmen, and continuing education of its nuclear professionals.

Established by the Nuclear Oversight Board, a governing body of USAF senior executives chaired by the secretary and chief of staff, the Air Force Nuclear Enterprise Flight Plan guides these initiatives. This publicly available document articulates the USAF's foundational understanding of the nature of deterrence and Airmen's role in providing the nation with nuclear deterrence capabilities.<sup>18</sup>

The USAF Chief of Staff, Gen Mark Welsh, has instituted a quarterly deterrence seminar for Air Staff principals. He leads this tabletop exercise, employing staff and outside expertise to consider various plausible near-future scenarios and debating contending solutions. USAF senior executives take this seriously, and their debates are frank, open, and sometimes contentious.

The curriculum of all USAF PME institutions is under vigorous review; new content and courses on twenty-first century nuclear deterrence are being introduced at every level. The Air Force Academy will soon offer several new courses supporting a new nuclear weapons and strategy minor for undergraduates. For all general officers and senior executives (even the chief of chaplains) there is now a senior leader course, "Nuclear 400," that engages participants in problem solving case studies of real-world deterrence operations and nuclear enterprise management




challenges. Nuclear professionals are required to complete weeklong continuing education courses to refresh and renew their expertise.

The Air Force LeMay Doctrine Center is bringing together nuclear deterrence professionals from all across the USAF to make a fundamental transformation of the nuclear deterrence operations annex to Air Force doctrine and to revise the treatment of deterrence across all elements of Air Force basic doctrine. In November 2014 the Air Force Studies Board of the National Academies concluded a two-year effort to develop a comprehensive plan for developing new methods, approaches, and tools for analyzing twenty-first century deterrence.<sup>19</sup> General Welsh directed the board's recommendations be implemented to enable USAF senior leaders to exert renewed intellectual leadership on deterrence.

America's Airmen know deterrence and are ready to articulate twenty-first century deterrence capabilities. The USAF has undertaken several activities and initiatives to reverse the lack of attention and interest that beset much of the DOD after the Cold War.<sup>20</sup> Moreover, the USAF will sustain its commitment and effort to deter extant and emerging nuclear threats in a post-Cold War world. *Myth #5 Busted—The USAF is not stuck in a Cold War mind-set—far from it.*

## Conclusion

Although the United States is committed to the goal of a nuclear-weapon-free world, as long as nuclear weapons exist in foreign arsenals, there is simply no alternative path for the United States than to maintain safe, secure, and effective nuclear capabilities. As a visible signal of our intent to act if circumstances warrant, the US bomber force remains crucial for extended deterrence of threats against allies and other partners during times of crisis. ICBMs, widely dispersed around three Air Force bases, are key for deterrence of attack against the United States, because for the foreseeable future no aggressor has any prospect of disarming our land-based missile force. Ballistic missile submarines patrol securely beneath the world's oceans, ensuring a secure second-strike capability even under the direst circumstances. With the commitment of resources, the unique attributes of each leg of the triad will continue to complicate adversaries' offensive and defensive planning and contribute to America's security.

Nuclear weapons played an essential role in preventing superpower war during the Cold War. Although the potential for major state-on-state war today may be lower, it is not absent and may indeed grow; therefore, USAF nuclear capabilities, as part of the US nuclear arsenal, continue to provide essential contributions to preserve the peace. Difficult decisions lay ahead, as the United States thinks about nuclear forces and nuclear deterrence. However, focusing on facts and applying sound reasoning can make the choices clearer. 

**James A. Blackwell Jr.**

Special Advisor to the Assistant Chief of Staff  
Strategic Deterrence and Nuclear Integration  
Headquarters, US Air Force

**Charles E. Costanzo**

Associate Professor of National Security Studies  
Air Command and Staff College  
Maxwell AFB, AL

**Notes**

1. David Chance, "U.S. Flies Stealth Bombers over South Korea in Warning to North," *Reuters*, 28 March 2013, <http://www.reuters.com/article/2013/03/28/us-korea-north-stealth-idUSBRE92R0DX20130328>.

2. Congressional Budget Office (CBO), *Projected Costs of U.S. Nuclear Forces, 2014 to 2023* (Washington, DC: CBO, December 2013), 2, <http://www.cbo.gov/sites/default/files/cbofiles/attachments/12-19-2013-NuclearForces.pdf>.

3. See Tom Z. Collina and the Arms Control Association Research Staff, *The Unaffordable Arsenal: Reducing the Costs of the Bloated U.S. Nuclear Stockpile* (Washington, DC: Arms Control Association, October 2014), <http://www.armscontrol.org/files/The-Unaffordable-Arsenal-2014.pdf>.

4. See Pres. Barack Obama's speech in Prague, Czech Republic, April 2009, [http://www.whitehouse.gov/the\\_press\\_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered](http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered).

5. William J. Perry, James R. Schlesinger, et al, *America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, DC: US Institute of Peace Press, 2009), xvi, [http://media.usip.org/reports/strat\\_posture\\_report.pdf](http://media.usip.org/reports/strat_posture_report.pdf).

6. *Ibid.*, xvii.

7. Amaani Lyle, "Stratcom Commander Outlines Deterrence Strategy," *American Forces Press Service*, 28 February 2014, <http://www.defense.gov/news/newsarticle.aspx?id=121751>.

8. Wendell Minnick, "US Report: China's Nukes Getting Bigger and Better," *Defense News*, 19 November 2014, <http://www.defensenews.com/article/20141119/DEFREG03/311190050/US-Report-China-s-Nukes-Getting-Bigger-Better>.
9. Bill Gertz, "China Tests ICBM with Multiple Warheads," *Washington Free Beacon*, 18 December 2014, <http://freebeacon.com/national-security/china-tests-icbm-with-multiple-war-heads>.
10. Kyle Mizokami, "The Dragon's Fire: Welcome to Chinese Nuclear Weapons 101," *National Interest*, 5 January 2015, <http://nationalinterest.org/blog/the-buzz/the-dragon%E2%80%99s-fire-welcome-chinese-nuclear-weapons-101-11968>.
11. Nuclear Threat Initiative, "Russia Test-Launches Two Strategic Missiles," *Global Security Newswire*, 2 January 2014, <http://www.nti.org/gsn/article/russia-test-launches-two-strategic-missiles>; and Tamir Eshel, "A Missile Testing Blitz Revamps Russian ICBM Modernization," *Defense Update*, 29 November 2014, [http://defense-update.com/20141129\\_russian\\_icbm\\_bltz.html](http://defense-update.com/20141129_russian_icbm_bltz.html).
12. Benjamin H. Friedman and Christopher A. Preble, "Ending Nuclear Overkill," *New York Times*, 13 November 2013, <http://www.nytimes.com/2013/11/14/opinion/ending-nuclear-overkill.html>; and Christopher Preble and Matt Fay, "To Save the Submarines, Eliminate ICBMs and Bombers," *Defense One*, 14 October 2013, <http://www.defenseone.com/ideas/2013/10/save-submarines-eliminate-icbms-and-bombers/71879/>.
13. Jonathan W. Greenert, "Payloads over Platforms: Charting a New Course," *U.S. Naval Institute Proceedings* 138, no. 7 (July 2012): <http://www.usni.org/magazines/proceedings/2012-07/payloads-over-platforms-charting-new-course>.
14. Naval Doctrine Publication 1, *Naval Warfare*, March 2010, 27, [https://www.usnwc.edu/Academics/Maritime--Staff-Operators-Course/documents/NDP-1-Naval-Warfare-%28Mar-2010%29\\_Chapters2-3.aspx](https://www.usnwc.edu/Academics/Maritime--Staff-Operators-Course/documents/NDP-1-Naval-Warfare-%28Mar-2010%29_Chapters2-3.aspx).
15. Perry and Schlesinger, *America's Strategic Posture*, 25.
16. *Ibid.*, 26.
17. See the remarks of Maj Gen Garrett Harencak, assistant chief of staff for strategic deterrence and nuclear integration at the US Strategic Command Deterrence Symposium in August 2014. US Strategic Command, "Panel 6 - 2014 Deterrence Symposium," *You Tube*, 19 August 2014, [http://www.youtube.com/watch?v=PFMtS4MhKyc&list=PLzO\\_KvP4phUYPNAqhWK\\_cDE73i7FteVQ5&index=10](http://www.youtube.com/watch?v=PFMtS4MhKyc&list=PLzO_KvP4phUYPNAqhWK_cDE73i7FteVQ5&index=10).
18. Eric K. Fanning and Mark A. Welsh III, *Flight Plan for the Air Force Nuclear Enterprise* (Washington, DC: Department of the Air Force, 26 June 2013), <http://www.af.mil/Portals/1/documents/news/FlightPlanfortheAirForceNuclearEnterprise.pdf>.
19. Committee on USAF Strategic Deterrence Military Capabilities in the 21st Century Security Environment, Air Force Studies Board, Division on Engineering and Physical Sciences; and the National Research Council, *U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods, and Approaches for the 21st Century Security Environment* (Washington, DC: The National Academies Press, 2014), <http://www.nap.edu/catalog/18622/us-air-force-strategic-deterrence-analytic-capabilities-an-assessment-of>.
20. Secretary of Defense Task Force on DOD Nuclear Weapons Management, *Report of the Secretary of Defense Task Force on DOD Nuclear Weapons Management, Phase II: Review of the DOD Nuclear Mission* (Washington, DC: DOD, December 2008), <http://www.defense.gov/pubs/pdfs/PhaseIIReportFinal.pdf>.

# Applying Cost Imposition Strategies against China

*Col Kenneth P. Ekman, USAF*

## Abstract

Cost imposition strategies focus on eliciting an adversary response that creates a hardship differential favoring the initiating nation. There is new interest in cost-imposing strategies as the most beneficial element of the competitive spectrum. If applied against China, cost-imposing strategies can succeed when based on correct predictions of Chinese responses and accurate accounting for the monetary and other security costs involved. In the air domain, competition involving China's ballistic and cruise missiles, surface-to-air missiles (SAM), and fighters offers the United States different degrees of advantage and hardship. Defense decision makers will find that cost imposition is not a panacea. They should understand the concept beyond its current level of misuse both for the disproportionate advantage it offers and for the liability it poses when used against America. To institutionalize the practice, the Department of Defense (DOD) should revive the competitive strategies structure and methods developed in the 1980s. Implementation will require overcoming institutional resistance, short time horizons, and significant fiscal constraints.



Over the last year, the potential to foist disproportionate peacetime military investment burdens on rival countries has sparked the inter-

---

Col Kenneth P. Ekman is commander, 8th Fighter Wing, Kunsan Air Base, Republic of Korea. He served in a variety of operational and staff assignments, including air component strategist and fighter analyst in the Office of the Secretary of Defense/Office of Cost Assessment and Program Evaluation. Colonel Ekman graduated from the USAF Weapons School, the Air Command and Staff College, the School of Advanced Air and Space Studies, and was an executive fellow at The Brookings Institution.

This article is a condensed version of Colonel Ekman's Federal Executive Fellowship Policy Paper, first published by the Center for 21st Century Security and Intelligence at The Brookings Institution in May 2014.



est of policy makers and defense practitioners alike. Think tanks like the Center for Strategic and Budgetary Assessments and the American Enterprise Institute have included cost imposition in their prescriptions for future US security strategies. Long-range planning efforts like the DOD *Quadrennial Defense Review* have also considered the approach.<sup>1</sup> Research and development agencies like Defense Advanced Research Projects Agency included the principle when considering new ways of achieving air superiority.<sup>2</sup> Senior military officers have used the term to characterize advantage and disadvantage relative to America's competitors.<sup>3</sup> Further, in his proposed amendment to House Resolution 4310, the National Defense Authorization Act for Fiscal Year 2013, Congressman Randy Forbes tasked the DOD "to conduct a study to identify cost-imposing/competitive strategies focused on countering potential challenges posed by foreign nations."<sup>4</sup> Hence, "cost imposition" is rapidly becoming today's strategic concept of choice, suggesting the possibility of attaining greater strategic advantage relative to US rivals.

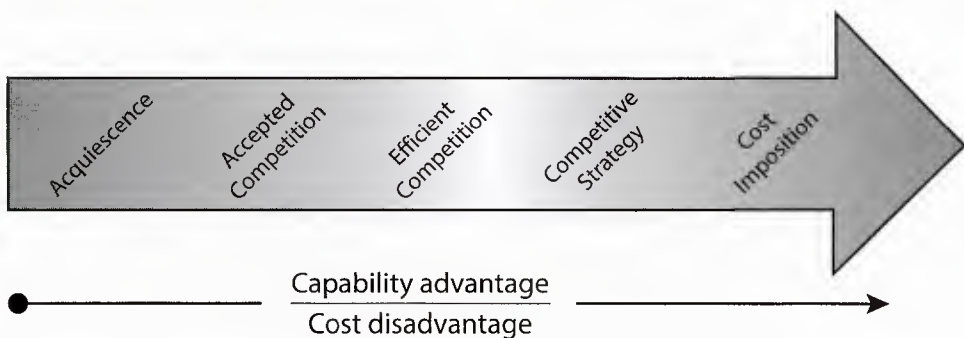
This article attempts to clarify cost-imposition methods for defense decision makers while applying them to a military competition with China. China's growing influence and aggressiveness appear threatening to US interests and allies in the Far East. Militarily, it has improved its capabilities to challenge US access and security guarantees, including general assurances in the Taiwan Relations Act. The military dimension of US-Sino relations is undeniably competitive, and opportunities for imposing costs upon China may exist as the competition unfolds. The argument begins by defining the concept of a cost-based competitive spectrum leading to cost imposition. It continues by accounting for the range of cost factors between security competitors and delves into *reacting opponent* responses, decisions, and choices linked to the *initiating competitor's* actions. Finally, it presents cost-imposition prospects inherent in key contests between US and Chinese air forces and suggests program, posture, and operating concept changes that could benefit America within each exchange.

## **Defining the Competitive Spectrum**

In a military sense, competition consists of a contest to create an advantageous differential in military capabilities, capacities, and perhaps options between rivals. Competitive strategy, as implemented by the

DOD in the 1980s, involved “aligning enduring American strengths against enduring Soviet weaknesses . . . to force the Soviets to perform less efficiently or effectively.”<sup>5</sup> Here cost imposition is defined as a more finely tailored competitive strategy whereby program, posture, and operational concept choices lead an adversary to incur greater hardship—fiscal or otherwise—through disadvantageous competition. These costs are incurred in peacetime though the relationship between prewar choices, and the ability to inflict or avoid damages in war should be considered, as the former sets conditions for the latter.

Yet, not every military competition is conducive to, or appropriate for, a cost-imposing approach. Identifying candidate areas for cost imposition involves less an either-or choice and more a correct assessment of where a capability standoff falls along the larger spectrum of military competition (*see* fig. 1). In this case, the competitor’s measure of effectiveness consists of the capability advantage created by the choice divided by the commensurate cost or hardship disadvantage. Contests where the competitor realizes less capability advantage or suffers more disproportionate costs fall further left on the spectrum. In some military strength comparisons, a competitor could *want* a rival to have greater strength.<sup>6</sup> These capability areas could include humanitarian assistance and disaster relief, nuclear weapons command and control, or internal security. Figure 1 depicts the resulting cost-based competitive spectrum, showing a trajectory leading to the best case though infrequent option whereby a nation can elicit an advantageous hardship differential from an adversary.



**Figure 1. Cost-based competitive spectrum**

From a direct investment perspective, *acquiescence* represents the cheapest and least capable cost-based competition. Here, the competitor chooses to allow an adversary's strength to go uncontested and saves resources in the process. Collective security agreements may permit the competitor to make this choice, as in the case of 25 nations that forego an indigenous nuclear capability while bandwagoning under the US nuclear umbrella.<sup>7</sup> In other cases, adherence to weapons-control regimes leads a nation to refrain from adopting certain capabilities like nerve agents, cluster munitions, and space weapons. Finally, the cost or adaptation required to field a competing or countering capability might simply be too much. The Soviets appear to have acquiesced when faced with the prospect of the US Strategic Defense Initiative. Unlike some of its extremist adversaries, the United States has chosen not to field a weapons system comprised of suicide bombers, though the DOD has taken other steps to mitigate this strategy. While acquiescence may appear to offer savings, the collateral costs required to compensate in other areas hardly make acquiescence a free option or an enduring choice. These include the autonomy ceded to join collective security agreements and the potential vulnerability of a competitor's vital interests in the event of conflict.

In a more active though costly approach, a nation could *accept competition* with a rival in a certain capability. Opting to compete creates further choices dealing with sufficiency. Reconciling an element of their military means with their security ends, competitors can compete to win, compete to achieve parity, or compete to create a lesser disadvantage. In setting this balance, a nation can elect to develop either a competing or a countering capability—or a combination of both.

Tradeoffs between quality and quantity and the Soviet conception of "correlation of forces" speak to the pursuit of *efficient competition*. The competitor could develop and operate a weapons system less expensively, as China's People's Liberation Army Air Force (PLAAF) was able to do by purchasing discounted fighter aircraft from the former Soviet Union in the mid-1990s.<sup>8</sup> Alternatively, a nation could enhance the system's effectiveness by employing superior operating concepts, such as the "initiative, innovation, and self-reliance" practiced by Western aircrews, providing them an advantage over their more numerous Soviet rivals.<sup>9</sup> The competitor could also develop and integrate new technologies, potentially delivering more capability for every dollar spent, as occurred in

the transition to precision-guided munitions. By partnering with other countries possessing complementary weapons systems, the nation can leverage additional capability and capacity. Furthermore, the competitor can shoulder reduced deterrent clout and additional risk should conflict occur by accepting disadvantage in the capability contest. Within the cost-based competitive spectrum, the majority of military rivalries appear to involve either accepting competition or competing efficiently.

The *competitive strategy* approach imparts a new level of effectiveness and efficiency, where a nation possesses an advantage while its rival is disadvantaged. In 1972, Andrew W. Marshall penned *Long Term Competition with the Soviets: A Framework for Strategic Analysis*, proposing that the United States was in a protracted contest with the Soviet Union for military strength, economic growth, and international influence. This realization prompted the national security establishment to focus on cultivating areas of military capability where America already possessed a distinct advantage over the Soviets through the method of competitive strategies.<sup>10</sup> The Reagan administration institutionalized the US-Soviet competition by creating the Competitive Strategies Office as an element of the Office of the Secretary of Defense and charged the organization with devising competitive initiatives vis-à-vis the Soviet Union. It functioned until 1991.<sup>11</sup> As a champion of the concept, Secretary of Defense Casper Weinberger claimed several American competitive strategy successes.<sup>12</sup> For example, he identified competitive success in antisubmarine warfare capabilities, made possible by US technological advantages in manufacturing, signals processing and acoustics, forward basing of these capabilities on the Soviet periphery, and submarine employment doctrine.<sup>13</sup> By choosing further investment in these advantages, the DOD elicited from the Soviets “disproportionate expenditures” to reduce the US threat to their submarine force.<sup>14</sup> As part of this response, Soviet conventional fleet design focused on defending areas close to the Soviet mainland, rather than projecting these forces long distances to threaten American assets in the US littoral.<sup>15</sup>

Within the spectrum, *cost imposition* represents the holy grail of military competition. Necessary preconditions include the requirement and will to compete, the impetus to do so efficiently, and the potential to do so from a position of capability advantage with ability and intent to elicit a disadvantageous response from an adversary. For the DOD, cost imposition should be waged within a larger framework of military



competition as an extension of competitive strategies. Successful cost-imposing strategies yield benefits offered by the range of competition types further left on the spectrum, while allowing the initiating competitor to endure less hardship than an adversary does.

In January 1966, Secretary of Defense Robert McNamara cited cost imposition against the Soviet Union as partial justification for acquiring bombers.<sup>16</sup> America leveraged its superior manufacturing, exterior lines offered by bomber bases both at home and abroad, higher quality aircrews, and lead in technologies including radar, navigation aids, communications, and—more recently—stealth.<sup>17</sup> The offensive, low-altitude, and low-observable threat these capabilities posed exploited Soviet paranoia. In response, the Soviet Union fielded over 10,000 SAM systems, numerous early warning and fire-control radar systems, tens of thousands of air-defense artillery systems, and at least 15 different major aircraft systems—many of which were single purpose interceptors.<sup>18</sup> One appraisal listed Soviet expenditures on SAMs alone at \$120 billion to protect the nation's 12,000-mile border.<sup>19</sup> The same group of authors asserted, "American investments in stealth and bomber aircraft in the 1970s compelled the Soviet Union to pay a substantially higher price to continue guarding its airspace from any intruder."<sup>20</sup> In the decade prior to the formal advent of the competitive strategies initiative, the Soviet Union's military expenditures exceeded those of the United States by 50 percent.<sup>21</sup> Through these investments, the Soviets attained substantial numerical superiority in a wide array of capabilities and were reducing their qualitative disadvantages as well. However, the successful US competitive strategy amounted to closing the military gap in effective and efficient ways that avoided "matching the Soviets tank for tank, ship for ship, or aircraft for aircraft."<sup>22</sup>

### **Accounting for Costs**

Cost imposition denotes a balance or calculus for gauging a differential in hardship between an initiating competitor and a reacting opponent. These costs can be monetary or less tangible, vary temporally from obsolescence to forward-looking, and create a range of consequences based on the economic strength and composition of each competitor. Clear accounting of costs becomes more important when predicting or assessing the relative advantage represented by hardship differentials.

The most obvious category includes direct investment costs associated with competing weapons systems. Such expenses would include development, procurement, operating, and modernization costs, as well as costs of associated armament. Using a fighter aircraft example, the imposition calculus would weigh direct investments in each competitor's fighter aircraft arsenal and associated weapons but would include only the portion of those fighter inventories most likely to be engaged in a direct confrontation between the competitors. While immediate program costs only capture a portion of the fiscal burden associated with specific weapons systems, a more comprehensive balance would include personnel costs, leading to consideration of individual service member productivity, unit manpower compositions and associated pay scales, and the broader array of military member entitlements and benefits.<sup>23</sup> Furthermore, a weapons system only comprises one ingredient of an operational capability. Better accounting would include program costs for enabling weapon systems. Going back to the fighter aircraft example, comparisons would include the personnel costs associated with operations and maintenance. Such accounting would also include costs of base support structures and maintenance depots, along with the expenses associated with the mobility, air refueling, and command and control platforms and networks necessary to organize, to train, and to equip the fighter force and to employ it in the security competitor's theater.

When facing a military capability threat, a rival nation can choose to field countering or asymmetric capabilities rather than directly competing technologies.<sup>24</sup> Oftentimes, this is not an either-or choice but rather a mix of competing and countering capabilities. Using the fighter force example, a rival nation could choose to compete via a modest investment in its fighter force, while favoring instead greater investment in SAMs and antiaircraft artillery. From a cost imposition perspective, countering capabilities can induce steep gradients in investment playing fields for all players. A countering capability fielded by a reacting opponent can change the entire calculus. The tendency would be for the counter, in lieu of the directly competing alternative, to be cheaper and thus more advantageous for the reacting opponent. A better measure of cost imposition might include costs of previously fielded systems made obsolete by new capabilities. Loss of utility for sunk costs may constitute an economic and security disadvantage to a competitor. When considering these costs, an imposition calculus will have to include some criteria

to discern between modicums of capability advantage associated with a typical arms competition spiral and fundamentally game-changing capabilities that truly marginalize the preceding capabilities they counter.

Recognizing areas where the United States is a target of an adversary's cost imposition efforts may provide new ways of thinking about how to reduce hardships through more efficient competition. Changes in how America develops, procures, and sustains weapon systems can improve the balance. Personnel and installation costs offer significant potential—as does divestiture of weapons systems—having little impact on already disadvantaged competitor choices. Sustaining long-standing postures benefitting previous competitions entails foregone present and future opportunities. Operational concepts that proved advantageous when confronting lesser competitors may elicit no beneficial response from a peer competitor and thus merit revision. For example, projecting land-based fighters from invulnerable bases and enabling them with tankers; command and control platforms; and intelligence, surveillance, and reconnaissance assets operating close to contested areas spurs few responses from China that benefit the United States. Indeed, insights provided by a cost imposition framework can be as useful in the losing exchanges they illuminate as in the opportunities they identify.<sup>25</sup>

Ultimately, monetary costs become relevant in a strategic sense only when placed in context of the national economies bearing them. Here, the scale and composition of each nation's economy becomes central. At one extreme, the United States can operate at a cost imposition disadvantage indefinitely against countries with small economies, simply because of its capacity to outspend them. These situations merely involve accepted competition where, at most, the United States could aspire to greater efficiency. With near-peer competitors like China, absolute investment costs must be placed in context and may be less relevant than percentages of gross domestic product (GDP) spent. In 2012, the United States spent \$646 billion on defense, equating to 4.2 percent of GDP.<sup>26</sup> At the same time, China spent approximately \$180 billion on defense, equating to approximately 2 percent of GDP.<sup>27</sup> Differences in total sums and percentages of GDP spent only approximate the hardship differential created by cost imposition. In the case of a global power like the United States, only a portion of the nation's spending involves competition with a particular opponent. One estimate attributes 35 percent of the DOD budget, or \$226 billion and 1.5 percent GDP, to Far

East force structure that could be used in a conflict with China, placing the United States and China much closer to spending parity in East Asia.<sup>28</sup> Where a security standoff ultimately leverages the will of each competitor's respective population, fiscal burdens at the national level comprise useful quantitative insights.

However, monetary costs only tell part of the story as they account for relative advantage. Cost-imposing strategies rely on fundamentally sound competition, waged efficiently, in a competitive strategies channel where the competitor enjoys an advantage. In the Soviet competitive calculus, quality and quantity of a particular force element were factored into a "correlation of forces" appraisal.<sup>29</sup> Capability and capacity have inherent value, as they constitute "hard power" strength before and during conflict. Better capabilities only loosely translate to military advantage, affected as they are by a nation's ability to adopt and wield them effectively.<sup>30</sup> The manner by which each competitor employs groups of weapons systems via operational concepts imparts relative advantage and inherent flexibility that cannot be valued in strictly monetary terms, nor can these factors be accurately assessed. Likewise, the countering or competing operational concepts an adversary develops in response bestow some degree of value to the other side of the balance.

Nobel-winning American economist Thomas C. Schelling acknowledged the challenge of bounding a cost-imposition calculus, observing that relative advantage is more easily determined when focusing on the narrow set of costs directly related to a specific capability contest.<sup>31</sup> He further noted that while accounting within a "suboptimization" was easy, the main thrust of cost imposition involves impacting investment choices occurring outside the area of competition.<sup>32</sup> Nevertheless, when one expands the scope of consideration, the more indeterminate the advantage becomes. Taken to the extreme, when the cost imposition balance grows to consider the entirety of international competition involved, "the best overall strategy, worked out in all its detail, is just the best strategy, all things considered; and any relevant costs have already been implicitly taken into account."<sup>33</sup> In the end, if the calculus is too narrow, it misses accounting for the hardships sought by the strategy. If the calculus is too wide, the accounting becomes indeterminate and of secondary importance to an overall appraisal of the competitors' relative security advantage.



The focus on monetary and other costs has a decidedly military bias. Broadly, security competitions and, more narrowly, cost imposition efforts necessarily employ all the instruments of national power. Diplomatic, economic, and information domains each provide their own opportunities for exacting hardships from a security competitor. Each domain possesses its own currencies that lend themselves to accounting and advantage determination to varying degrees. As with any security confrontation, the competitor most likely to win will be the one that effectively harmonizes all these instruments, in part through understanding the real exchange ratios of the various types of currencies involved. Command economies and artificially set exchange rates make this determination even more difficult.

The challenge for defense decision makers involves determining which costs will and will not be considered in an imposition calculus. A collective understanding of a competitor's national economy, defense spending, and methods of employing military capabilities will influence the choices. Selections made to create cost imposition advantage should include clear identification of the expected costs associated with the primary and alternative responses elicited. Practical limitations of insight and time will drive boundaries drawn for considered costs, which will involve some artificiality. Strategists and planners should elevate the discussion beyond comparisons of the cost of one antiship cruise missile to the cost of an aircraft carrier, moving instead to a comparison of the systemic costs of those opposing capabilities. Certainly, in defense circles no straightforward answer attends the question, "How much does it cost?" Valuation of cost imposition balances will be no easier.

Finally, the DOD should carefully consider both the reliability and vulnerability of the collective security partners affected by a cost-imposing strategy.<sup>34</sup> When a strategy relies on the capability contributions of one or more allies, the United States should proceed only with the reasonable assurance that partners will make good on their future contributions—lest the desired hardship differential be diminished. When designing a cost-imposing strategy excluding partner contributions, the DOD should still gauge the potential for collateral damage resulting from the ensuing bilateral capability contest. While collective security arrangements can significantly exacerbate the hardship differential in America's favor, the intricacies of each partner's decision calculus should

be understood to prevent costs being placed back on the alliance leader and to preclude fracturing the alliance itself.

## Gauging Adversary Response

Prospects for cost-imposing strategies depend on defense decision makers' success in anticipating an adversary's response to a DOD program, posture, or operating concept choice. Absent understanding of a nation's intentions behind a competitive choice, it is difficult to make judgments regarding which choices were failed strategies and which choices were further left on the competitive spectrum. A variety of cause and effect relationships informs international security relations and how they could enable cost-imposition attempts into potential points of leverage. Even when the opportunity exists, going forward with a cost imposition strategy may not yield benefits and may actually do more harm than good. Certain arms race tendencies or crisis stability concerns could restrain cost-imposition attempts. Unfavorable differences in adoption capacity between the initiating competitor and the reacting opponent could also prompt inaction. In situations where the competitive choice is less likely to elicit the desired reaction and alternative reactions carry greater disadvantage, the competition should end. Furthermore, if a cost-imposition strategy is to sharpen rather than diminish a nation's competitive edge, decision makers should consider several contextual variables.

The initiating competitor should have reasonable confidence that the reacting opponent perceives itself in competition in the selected capability area. In absence of an opponent's commitment to compete, the initiating competitor's choices are unlikely to elicit the desired reaction. This situation leaves the initiating nation incurring all the additional costs and likely results in a hardship differential that favors the reacting opponent. Particularly at the outset of a cost-imposing strategy, the initiating competitor should gauge the likelihood that the increased competition will prompt the opponent to react in overt conflict. A new, surprising, or highly disadvantageous hardship differential could fan the embers of a latent *casus belli* between the two competitors. Arms race theory warns that conflict is most likely at the outset of the race.<sup>35</sup> In their book, *Strategic Reassurance and Resolve*, authors James Steinberg and Michael O'Hanlon repeatedly caution against the destabilizing effects an arms race between the United States and China could have.<sup>36</sup> While carefully

managed arms races may actually contribute to crisis stability and conflict avoidance, they likely derive their stability from clear mutual understanding between competitors reinforced by control regimes. When an arms control agreement limits each competitor's maximum defense investment or fixes their respective investments by prescribing a ratio, the monetary context becomes zero-sum. When an adversary reacts by spending to shore up a weakness, other capability areas must suffer because the adversary cannot increase the quantity of resources available for defense. Steinberg and O'Hanlon propose instituting a two-to-one military spending ratio for the United States and China, respectively.<sup>37</sup> While their main intent is to limit an overall arms race between the countries, such an agreement could increase the likelihood that cost-imposing strategies would exact greater hardship differentials and yield more competitive advantage. Thus, the existence of and mutual adherence to arms control agreements can increase cost-imposition efficacy. Because of the conflict risks they pose, when the relationship between two competitors appears precarious, cost-imposing strategies are better left unwaged, regardless of the hardship differential returns they offer.

Another dangerous opponent reaction would witness an unforeseen technological breakthrough coupled with the financial intensity and organizational capital to adopt it. This breakout alternative reaction could change the competition, placing the initiating nation at a disadvantage. A sound assessment of the opponent's research and development enterprise can help mitigate this outcome, as would pursuit of similar innovation by the initiating competitor. Opaque societies make this appraisal more difficult. As an example, the commander of US Pacific Command stated in October 2009, "In the past decade or so, China has exceeded most of our intelligence estimates of their military capability and capacity, every year."<sup>38</sup>

## **Decision Theories and Competitor Choices**

While multiple theories like rational decision, deterrence, spiral, and arms control cast each competitor as monolithic and perfectly perceptive of the external environment, Robert Jervis disaggregates competitors and injects more potential for fallibility. He posits that decisions are made by inherently flawed people, that competitors should be disaggregated to allow multileveled analysis, and that decisions occur in

the “fog of foreign policy making” due to varying degrees of perception and misperception.<sup>39</sup> Therefore, competitor choices become products of complementing or competing interests at decision-maker, bureaucratic, domestic political, and international environmental levels.<sup>40</sup> Furthermore, competitors make choices based not only on their perceptions of the security environment but also on the “evoked set” of concerns and information dominating one or more of these factions’ cognizance at the time of the decision.<sup>41</sup> Theories like Jervis’s help spur defense decision makers to better understand a security competitor’s intentions, predispositions, and decision-making processes before selecting cost-imposing strategies. Recognition that even the deepest of understandings can still yield suboptimum choices is inherent to this degree of insight.

Alternatively, some capability challenges go unanswered. One riddle of US-Sino competition queries why, despite America’s significant submarine capability advantage and the impact this force would have in any conflict between the two nations, China has refrained from developing a significant antisubmarine warfare (ASW) capability vis-à-vis the United States.<sup>42</sup> China employs its diesel attack submarines (SS) for coastal defense, offensive mine warfare, and as local sources of intelligence.<sup>43</sup> Chinese SS capabilities are appropriate to counter diesel submarines operated by potential regional adversaries but have limited to no capability against American nuclear attack and ballistic missile submarines, the most difficult ASW targets.<sup>44</sup> Furthermore, the littoral focus of very limited Chinese ASW capabilities involves operating in poor acoustic conditions present in the Yellow, East China, and northern South China Seas; whereas, US submarines have the ability to maneuver at will in Chinese coastal waters.<sup>45</sup> Moreover, China does not appear to be making any major investments to improve its ASW force.<sup>46</sup>

Following the advent of a significant military innovation, competitors may or may not choose to exploit it. Political scientist Michael Horowitz characterized competitors’ ability to respond as adoption-capacity theory, stating that “once states have the necessary exposure to an innovation, the diffusion of military power is mostly governed by . . . level of financial intensity required to adopt . . . and the amount of organizational capital required to adopt.”<sup>47</sup> Adoption-capacity theory explained otherwise anomalous responses to military innovations and provided insights supporting better imposition choices. For example, the theory explained why—despite the 70-year existence of nuclear weapons—only



13 states adopted the technology, highlighting the financial intensity involved in developing and sustaining a nuclear weapons program.<sup>48</sup> Rather than compete or counter, competitors may elect instead to harness the capabilities of a third-party nation, deferring substantial costs. When financial intensity or organizational capital precludes adoption, bandwagoning is an alternative response to the emergence of a military innovation.<sup>49</sup> For example, by bandwagoning under the US nuclear umbrella, 25 North Atlantic Treaty Organization (NATO) nations have foregone the financial intensity of developing indigenous nuclear weapon capabilities. The same recourse occurs in the case of mature, conventional capabilities. Collective defense alliances like NATO allow member nations to forego or share significant financial burdens, benefiting the cost-imposition balance relative to the alliance's security competitors. Foreseeable competitor responses to US cost-imposition attempts should include the bandwagoning option and address the counterreactions the United States would apply in response.

As a corollary, the United States has opportunities to leverage the investments and capabilities of its allies in a way that tilts the cost-imposition balance to its advantage. Direct military aid to allied nations provides a net capability increase while reducing US expenditures on costs such as manpower, installations, and enabling capabilities. Relatively inexpensive theater security cooperation bolsters both the capability and interoperability of allied militaries—thus, imparting a new slope to the balance of forces. Foreign military sales improve interoperability. They also provide an economic boost to US companies, while denying sales, economies of scale, and associated interoperability benefits to a competitor. However, third-party consideration can also constrain otherwise advantageous cost-imposing strategies. Fielding an improved weapons system or posturing a capability in a particular location may prompt an opponent's response, placing allies at further disadvantage. This predicament would effectively constitute cost-imposition collateral damage. Because of a competitor's choice, allies bear increased hardship in their attempts to reset the balance. Thus, the primary and alternate responses of allied nations, particularly those proximate to a competitor, become essential considerations when developing cost-imposing strategies. At best, complimentary allied responses can further tip the cost-imposition balance against the opponent. At worst, allies could abdicate for finan-

cial intensity or organizational capital reasons and either adopt a neutral stance or bandwagon with a US rival.

Theorists acknowledge to a varying degree uncertainty in eliciting a desired reaction from a competitor. Specifically on the subject of cost imposition, Schelling argued that small differences in a reacting opponent's demand for a capability can create large differences in the actual response.<sup>50</sup> The presence of "demand elasticity" creates the situation where a competitor's action cannot reliably elicit the intended reaction, which in turn decreases the likelihood of creating a favorable hardship differential.<sup>51</sup> Unpredictability makes the loop of assessment, feedback, and adjustment a critical element of successful cost-imposing strategies. An additional consideration driving cost imposition deals with the degree to which program, posture, or operational concepts affect crisis stability between competitors. The history of nuclear arms competition includes several cases where a new capability introduction, change in force posture, or revised operating concept bolstered deterrence but made the path to conflict more likely and more difficult to arrest.<sup>52</sup> As an example, in the mid-1960s Secretary of Defense McNamara chose to field multiple independently-targetable reentry vehicles (MIRV) on US submarine- and land-based missiles as a competitive counter to predicted Soviet antiballistic missile capabilities.<sup>53</sup> This choice produced a first-strike incentive and reduced crisis stability between the two nations, an unintended effect that took over 30 years to remedy.<sup>54</sup> In a conventional sense, long-range, highly destructive, one-time use systems lack the ability to perform proximate, graduated, tit-for-tat escalating operations. While America tends to favor the offensive as a power-projecting nation, defensive systems can stall an opponent's initial attack and provide intermediate options between peace and full-scale conventional conflict.<sup>55</sup> Ultimately, decision makers must consider cost-imposing choices yielding prewar opportunities in light of the degree to which these options help or hurt US flexibility to respond in an advantaged but graduated manner should hostilities commence.<sup>56</sup> Therefore, when focused by clear understanding of how the interaction between the competitors may unfold, a cost-imposing strategy has greater probability for success. Sun Tzu famously counseled strategists to know their enemies and to know themselves.<sup>57</sup> By understanding the complexities of cost-imposition interactions, decision makers may refine the discussion and make more successful choices.

## **Cost Imposition and China**

Over the last two decades, China's defense spending has increased by an annual average of 11 percent in real terms and at a rate slightly more than China's GDP growth.<sup>58</sup> By 2020 China's defense spending will likely approach \$300 billion, while US defense spending will likely remain close to \$550 billion.<sup>59</sup> By 2030, China's budget could reach \$500 billion, based on GDP projections.<sup>60</sup> Within these timeframes, the United States and China will come much closer to military spending parity than the current balance suggests. China's rapid economic and military rise, investments in capabilities that thwart US regional security guarantees, and aggressive sovereignty claims signify ongoing competition with the United States. Since the 1990 Gulf War, and particularly after a successful US deterrent response in support of Taiwan in 1995–1996, China has aggressively sought to nullify US military advantages in the Far East.<sup>61</sup> However, the United States is late even to acknowledge the competition exists, partially due to preoccupation with campaigns in Iraq and Afghanistan.<sup>62</sup> Not until 2012 did the Obama administration identify the need to rebalance toward the Asia-Pacific, and only in November 2013 did National Security Advisor Susan E. Rice describe “managing [the] inevitable competition” with China.<sup>63</sup> Especially in the case of China, the US defense establishment clearly recognizes the potential value of cost-imposing strategies. When opportunities exist to impose costs, the DOD should impose them via program, posture, and operational concept choices offering the most lucrative hardship differentials.

## **A Framework for Competing with China**

In their article, “U.S.-China Balance in a Three Game Framework,” David Frelinger and Jessica Hart suggest the military balance between the two nations, and particularly the implications of the PLA's modernization, can be assessed within three different game frameworks: influence, third parties, and power.<sup>64</sup>

Each of these frameworks involves a different scope, which in turn invokes different strategic ends along with alternate competitive ways and means to achieve them. The game of influence involves largely political competition—with the military in a supporting role—for influence and primacy in a variety of regions. For the United States, this region may

be global, while for China, the focus may be narrow and consist of the Taiwan Strait and the South and East China Seas.<sup>65</sup> Secondly, the battle over a third-party game largely emphasizes the military power balance, as it would affect conflict over a third nation or over that nation's key interests. Stakes in this game can be highly asymmetric, with one competitor ascribing greater importance to control of the third party. This asymmetry of stakes and interests also makes armed conflict over disputes unrelated to the third party highly unlikely.<sup>66</sup> Thirdly, the great power game has the broadest scope and highest stakes, leading to valuing every interaction between two competitors within a zero-sum calculus.<sup>67</sup> Regardless of which game ultimately best typifies US-Sino relations, cost imposition offers potential benefits if well played.

The entire concept of competitive strategy inverts the more traditional approach to building military power. The strategy focuses more on the reacting opponent than on the United States. Rather than countering opponent strengths, the strategy exacerbates opponents' weaknesses. In the three-move process, the goal is to elicit a specific adversary reaction. The action taken by the United States is secondary and may require adjustment. When the adversary displays an unexpected reaction, increased investment in previous choices would further entrench an obsolete action while foregoing a more appropriate counterreaction.

A measured competitive framework in the military domain against China could be one that emphasizes Frelinger's and Hart's battle over a third party. This approach acknowledges the asymmetries of national interest and constrains the military balance to proximate forces and those likely brought to bear in the event of conflict. It would localize the contest in the areas bounded by the South and East China Seas, Taiwan and the Taiwan Strait, plus eastern portions of mainland China. The competition would remain largely beyond reach of US territories and compel China to make further investments in primarily defensive programs, postures, and operating concepts. The conditions are largely set for an air component arms race specifically focused on fighter aircraft and armaments, where the United States need only preserve its advantage while emphasizing quality over quantity. A lesser game of influence can be played in other regions of the world, where US capabilities and experience can eclipse China's peacekeeping, humanitarian assistance, and disaster response initiatives. Other activities, such as dealing with piracy off the Horn of Africa, will offer opportunities for US-Sino coop-



eration, decreasing the likelihood that the battle over a third party will result in conflict.

While opacity characterizes many aspects of Chinese foreign policy decision making, several insights clearly offer competitive strategy leverage to the United States. China's evoked set of concerns deals with defense of the homeland, a constant in the country's expansion of comprehensive national power within its twenty-first century "strategic window of opportunity."<sup>68</sup> China's leaders "view a modern military as a critical deterrent to prevent actions by outside powers that could damage Chinese interests, or to allow China to defend itself against such actions should deterrence fail."<sup>69</sup> The ability to prevail in a conflict over Taiwan—largely a conflict wherein China defends its territorial and governance claims—has dominated the People's Liberation Army's (PLA) force modernization agenda for the last 15 years.<sup>70</sup> While the 2008 defense white paper commends a shift towards active defense and a better balance of offensive and defensive capabilities, these efforts largely amount to holding would-be aggressors at greater distances.<sup>71</sup>

Multiple factors suggest that first and foremost, the United States could leverage competitive and cost-imposing strategies against China in the air domain. Air capabilities have increasingly become the military foreign policy tool of choice. In fact, in the last six years China has even developed a "ladder of intensity levels" for deterrence using conventional air and space forces, including ballistic and cruise missiles, SAMs, and fighter aircraft.<sup>72</sup> Foreseeable conflicts with China would largely occur in the air and sea domains encompassing the Taiwan Strait, the South China Sea, and the East China Sea.<sup>73</sup> The United States and its close allies have no contiguous borders with China supporting large-scale employment of land forces. Furthermore, the limited US aims supporting peace and stability for people on Taiwan and reluctance to conduct large-scale land operations make land force investments a less lucrative choice.

### **Interacting with China and the PLAAF**

Competition in the air with China involves a contest with the PLAAF. The better strategies will be those that account for the PLAAF's stature as a component of the PLA, its history and perceptions, and the people the PLAAF employs. Several attributes distinguish the PLAAF as a particularly attractive target for competitive and cost-imposing strate-

gies within the larger US-Sino competition. As with greater China, the PLAAF nurtures an evoked set of sovereignty concerns borne out of its long-standing defensive orientation. PLAAF leaders and initiatives have limited influence within the larger PLA, making the air force less able to react effectively due to bureaucratic constraints.<sup>74</sup> Furthermore, defense analyst Kenneth Allen contends that the enduring pattern of army domination within the PLA will continue through the next decade.<sup>75</sup> Cultural and force-structure factors further exacerbate the PLAAF's disadvantage relative to the US Air Force (USAF). The PLAAF has had no significant combat experience since the 1958 Taiwan Strait crisis, placing the service over half a century behind US air forces.<sup>76</sup> Subsequent limited engagements of US forces during the Vietnam War provided grounds for a flawed service tradition wherein the PLAAF esteems itself as the only air force ever to have defeated the USAF.<sup>77</sup> By its own admission, the PLAAF needs to improve considerably its capabilities, doctrine, and training to challenge US power-projection capabilities.<sup>78</sup> While initiatives prompting these needed changes are ongoing, the PLAAF will continue to compete from a position of disadvantage relative to the USAF in the interim. Key Chinese air capabilities warranting deliberate competition include ballistic and cruise missiles, SAMs, and fighter aircraft.

### **Chinese Ballistic and Cruise Missiles versus US Air Defenses**

One capability contest that bears examining for its current location on the cost-based competitive spectrum and its poor potential for offering cost-imposing opportunities involves Chinese ballistic and cruise missiles and US defensive measures. From an American perspective, the contest currently amounts to accepted competition in pursuit of reduced disadvantage. As of December 2012, China had deployed more than 1,100 short-range ballistic missiles opposite Taiwan.<sup>79</sup> While Taiwan possesses 22 SAM sites, with a mix of long- and medium-range systems, only three Patriot PAC-2 batteries have any counter-ballistic missile capability.<sup>80</sup> One RAND study estimated that about 60 to 200 Chinese short-range ballistic missiles could neutralize most of Taiwan's fighter bases, and additional missiles could effectively suppress Taiwanese air defense operations, allowing employment of PLAAF strike aircraft.<sup>81</sup> Land-attack cruise missiles launched by H-6 bombers and longer-range ballistic missiles like the DF-21/CSS-5 can extend the reach of PLAAF

missile attacks far beyond Taiwan to Okinawa, other bases in southern Japan, aircraft carriers at suitable employment distances from the Strait of Taiwan, and even Guam.<sup>82</sup> The range, numbers, and destructive effectiveness characterizing China's relatively inexpensive missile force denies the United States and its allies the ability to stage fighter operations from sanctuary in support of a Taiwan crisis.

Successful active defense against Chinese missiles is difficult and costly. While relatively effective against individual missile attacks, Terminal High Altitude Air Defense (THAAD) and Aegis Ballistic Missile Defense units protect small areas and could be overwhelmed by mass attacks. These systems are expensive. For example, each THAAD battery costs approximately \$800 million.<sup>83</sup> Each Aegis Ballistic Missile Defense Ashore battery, a land-based variant, also costs approximately \$800 million.<sup>84</sup> Fielding sufficient systems to protect key military and strategic locations vulnerable to Chinese attack is simply cost prohibitive. As an alternative, measures improving resilience provide protection and enable continued operations despite even large-scale, coordinated attacks.<sup>85</sup> They also can invoke a spiraling competition involving adversary missile numbers, accuracy, and munitions effects. Dispersal complicates Chinese missile targeting and may reduce attack densities per location, but limited sites support dispersed US fighter operations due to the runway length and composition, munitions, and fuel access. Increasing US air forces' standoff distances can render obsolete many Chinese missile types, but the locations of Taiwan and other US allies remain interminably fixed and close. Camouflage, concealment, and deception, along with hardening aircraft, personnel shelters, and key infrastructure can improve survivability. Furthermore, programs and operating concepts allowing better indications and warning and enabling faster and more robust military installation recovery mitigate ballistic and cruise missile attacks.<sup>86</sup> Nevertheless, the United States and its allies cannot defend everywhere against everything, cannot fully recover from every attack, and cannot endure the financial intensity of trying to do so.

While America's prospects of fully protecting its air forces and its allies against Chinese missile capabilities are poor, competitive improvements remain possible and may reduce US capability disadvantage and hardship. This competition may amount to foiling a Chinese competitive strategy that threatens to impose excessive costs on the United States. An appropriate American counter should consist of efficiently competing

from disadvantage while searching for alternative approaches to undermine China's capabilities, postures, and operating concepts. The following choices support these ends:

- **Programs**—Harden threatened US installations sufficiently to make some conventional missile munitions and submunitions obsolete, creating a spiral of US hardening and Chinese obsolescence. Develop dispersed operating locations. At main operating bases, construct redundant runways and taxiways. Field robust airfield repair equipment and backup systems delivering essentials like fuel and electricity.
- **Postures**—Field ballistic missile defense systems at key US bases. Balance forces postured inside and outside PLAAF intermediate missile ranges. Encourage allies to acquire more ballistic missile defense systems, preferably by buying or coproducing US models.
- **Operating concepts**—Reduce Chinese missile targeting effectiveness. Improve ability to counter air-launched cruise missiles, both before and after launch. Assess US capability to destroy or suppress ballistic missiles prior to launch. Improve attack recovery practices.

### **Chinese SAMs versus US Strategic Attack**

An improved understanding of the PLAAF illuminates both the opportunities and limitations associated with the competition between Chinese SAM systems and American strategic attack capabilities. The PLAAF's commitment to defensive systems suggests that it will respond aggressively to future US offensive capability enhancements. The nature of this particular military competition makes pursuit of US advantage both expensive and tenuous. Where this competition falls along the competitive spectrum in the future is not predetermined and will be heavily influenced by future US choices.

True to its defensive heritage, the PLAAF has invested heavily in advanced SAMs, rendering its perimeter much less penetrable by US aircraft and munitions. These defenses hold American air assets at greater distances, placing US strategic attack assets at a competitive disadvantage in any conflict in the Chinese littoral. "US bombers carrying cruise missiles might be compelled to launch farther from the Chinese coast," limiting their missiles' reach.<sup>87</sup> Chinese SAMs would also constrain non-



stealth US fighters, which “would be greatly at risk if called upon to fly within the S-300/400’s envelope.”<sup>88</sup> The range and capabilities of these systems would further constrain efforts to suppress or destroy them using munitions delivered from the air.

While the current balance of forces may amount to an American competitive disadvantage, that balance may retrospectively constitute a competitive and even cost-imposition victory. These defensive systems pose no direct threat to the United States, though they significantly affect the battle over a third party. SAM systems are expensive, with one source citing the cost of an unspecified S-300 variant battery at \$115 million, plus \$1 million per missile.<sup>89</sup> Meanwhile, the United States has made few investments directly serving this competitive facet vis-à-vis China. America’s small bomber fleet—consisting of 74 B-52s, 62 B-1s, and 20 B-2s—has multiple nuclear and conventional purposes.<sup>90</sup> Within its foreseeable uses, a US-Sino conflict is but a subset. The stealthy B-2 has inherently greater capability in the face of Chinese defenses, as do stealth fighters like the F-22 and F-35—though these fighters’ range limitations necessitate closer proximity and air refueling. Fighters are also less able to penetrate deep into China’s interior. On the whole, China has spent heavily over the last two decades to counter US strategic attack systems that were primarily focused elsewhere.

Looking forward, the DOD may not have the opportunity to impose a similar degree of costs within this contest. Accepted competition for parity or advantage will require the United States to make additional investments to modernize its strategic attack capabilities, while the long-range strike bomber capable of performing some or all of these functions may improve the US competitive edge. However, with a program cost exceeding \$100 billion to achieve a planned force structure of 80 to 100 aircraft, the Long-Range Strike Bomber (LRS-B) may not enable the United States to impose an advantageous hardship differential regardless of the response the program elicits from the Chinese.<sup>91</sup>

Opportunities may exist to compete more efficiently. Some trade space may exist between the F-35, LRS-B, and standoff munitions programs to achieve a more competitive and efficient balance tailored to the battle over a third party. Alternative conventional strike approaches, such as improved air-launched munitions or sea-launched munitions like those from the US Navy’s *Virginia*-class Payload Module can also improve efficiency but will have to be traded against the flexibility, range, and

persistence that may be inherent to the LRS-B. Where practicable, the United States should encourage third parties to field and sustain organic strategic attack capabilities.

Optimistically, the DOD might be able to leverage a competitive strategy in this contest while improving its forces' abilities to defeat Chinese SAMs and operate in areas protected by these systems to conduct conventional attacks deep in China's interior. PLAAF SAM investments show China's penchant for defense. In fact, a long-time China observer noted, "the Chinese armed forces are obsessed with defending China from long-range precision air strikes" and, therefore, invested heavily in passive defense capabilities provided by hardened and deeply buried facilities.<sup>92</sup> Chinese writers have expressed concerns about space planes' "global reach, information sharing, and precision strike capabilities."<sup>93</sup> Like stealth technology, the speed of such craft effectively reduces the engagement envelope of Chinese SAMs. Furthermore, while Chinese SAMs ostensibly could operate in defensive concert with PLAAF fighters, a dearth of information currently exists as to how the PLAAF operates these defensive forces together.<sup>94</sup> With some technological and financial intensity preconditions, opportunities may still exist for the DOD to elicit disadvantageous, defensive Chinese responses to future competition in the realm of US strategic attack. These considerations lead to the following choices as potential ways to shift the contest further right on the competitive spectrum:

- **Programs**—Balance F-35, LRS-B, and standoff munitions resources to more efficiently serve conflict scenarios with China. Develop and field survivable, long-range munitions capable of striking Chinese target sets at less cost. Encourage partners and allies to field their own capabilities. Improve US abilities to suppress and defeat Chinese SAMs.
- **Postures**—Pursue a frontier basing strategy, making a portion of available Asia-Pacific airfields suitable for supporting bomber operations close enough to China to enhance deterrence and responsiveness but outside the range of most Chinese conventional offensive capabilities.<sup>95</sup>
- **Operating concepts**—Assess and exploit PLAAF weaknesses in conducting integrated SAM and fighter engagement zones. Train

with allied air forces to improve their capabilities and interoperability with US forces in defeating Chinese SAMs.

### **Fighter Aircraft Competition**

The ongoing US-Sino competition in fighter aircraft bears examining for several reasons. First, depending on the timeframe considered, the United States can claim or achieve varying degrees of hardship advantage or disadvantage. Next, fighter aircraft capabilities are expensive and complicated. The F-35 is the most costly and ambitious acquisition program ever, with total acquisition costs approaching \$400 billion.<sup>96</sup> Finally, this competition can be susceptible to countering capabilities—both within and outside fighter technologies—that may induce large shifts in relative competitive and hardship advantage.

China's fighter aircraft modernization effort from 1995 to 2010 may represent a competitive and cost-imposition success for the United States that will be more difficult to continue in the upcoming period of USAF modernization. In this period, the PLAAF divested 3,500 aircraft, while procuring 399 fourth-generation fighters and at least 250 modernized third-generation fighters.<sup>97</sup> Meanwhile, the USAF divested approximately 970—most with capabilities rivaling newer Chinese aircraft—and procured only 266 fighters during a period colloquially called a “procurement holiday.”<sup>98</sup> While the USAF's divestiture was not influenced by competition with China and procurement only partially so, the Chinese bore tremendous direct procurement and obsolescence costs in the PLAAF's attempts to modernize primarily vis-à-vis the USAF. From a cost-imposition perspective, China's introduction of the J-20 and J-31 prototypes bodes well, as they represent early milestones in a long, costly road to developing and fielding fifth-generation fighters. Meanwhile, the USAF's F-22 fleet has matured since initial operational capability in 2005, and the one hundredth F-35 was produced, though at no small cost.<sup>99</sup>

China has attempted to mitigate America's qualitative advantage by countering with “informationization” or electronic countermeasures (ECM).<sup>100</sup> It “gained immense benefit from its extensive access to Russia's EW [electronic warfare] designers and manufacturers, whose business was sustained by Chinese orders over the long period.”<sup>101</sup> China acquired Russian Sukhoi Su-27SK and Su-30MKK fighters, with their associated state-of-the-art jammers and countermeasures pods.<sup>102</sup> The

Chinese domestically produced J-11B carries an ECM pod resembling Russian designs, and the J-10B will likely feature an advanced radar, capable of functioning as a more powerful jammer.<sup>103</sup> These counter-measures could reduce the capability of and even neutralize current US fighters' radars and radar-guided missiles.

Several factors make US-Sino fighter-aircraft competition ripe for American competitive strategy. Few weapon systems require successful integration of as many diverse high-end technologies as do fighters, and the Chinese are currently 15 to 20 years behind the United States.<sup>104</sup> Though in the past the PLAAF acquired its aircraft by either purchasing or coproducing them, China's violation of the terms of its indigenous production agreements with Russia involving the SU-27 led to a 2006 Russian refusal of further military aviation sales, leaving China short of aircraft suppliers.<sup>105</sup> China now has to produce its own airplanes and, in doing so, is likely to incur more costs associated with development and manufacturing than China bore when purchasing Russian hardware in the mid-1990s. Since its inception, the PLAAF has been a fighter-centric force and shows no signs of willingness to accept a balance of forces deficit relative to the United States in East Asia. Thus, for the PLAAF, the apparent imperative will be to spend heavily to match the United States.

Though China has willingly borne the financial intensity associated with adopting modern fighter technologies, it remains to be seen whether the PLAAF can expend the organizational capital. Operationally, the PLAAF has yet to make the transition to a centralized control and decentralized execution method of employment that has garnered such success for Western air forces.<sup>106</sup> The ongoing transitions from purely defensive to the full spectrum of offensive to defensive tactics and from a purely air-to-air to multirole mission will heavily tax the PLAAF's organizational capital.<sup>107</sup> Autonomy exploited in US fourth-generation tactics has not been infused in PLAAF employment. Furthermore, stealth aircraft diffusion via the J-20 and J-31 will require significant PLAAF employment and sustainment adaptations.

The United States is winning the fighter-aircraft competition with China. Retrospectively, the DOD elicited a Chinese response likely representing a hardship differential advantageous to the United States over the period of 1995 to 2010. Looking forward, the United States has the opportunity to wage a successful competitive strategy, though



the financial intensity associated with air force fighter recapitalization may inhibit favorable cost imposition. At the same time, the predominately fifth-generation US fighter force represented by the F-35 may make Chinese fighter investments to date merely obsolescent costs. The United States may preserve much of its advantage through the following choices:

- **Programs**—Field the F-35 in sufficient numbers and sustain the F-22 to prompt continued Chinese fifth-generation fighter development and fielding. Looking forward, the United States should continue developing a follow-on to these aircraft to make obsolete an even greater portion of the Chinese fleet. The DOD should procure fighters more efficiently. Inadvertent technology hemorrhage to China should be minimized. The size of the DOD fighter force should support bringing to bear a stressing number of US fighters in any crisis with China. Explore disruptive technologies in air-to-air missiles.
- **Postures**—Maintain adequate fighter presence in the Far East to provide immediate support to a broad range of response options during any US-Sino crisis. Prioritize Far East bases for F-35 or F-22 bed down as the US fifth-generation fleet grows. Encourage allies to acquire competitive fighters, preferably by buying or coproducing US models capable of networking with US systems.
- **Operating concepts**—Improve US effectiveness in countering Chinese fighters, particularly in an informationized environment. Research and test alternative ways to neutralize Chinese fighters—both when airborne and prior to launch. Train with allied fighter forces to improve their capabilities and interoperability with US forces.

### **Bounding Challenges in US-Sino Competitions**

The three specific US-Sino competitions for the air domain bear revisiting. In each case, drawing boundaries to clarify competing or countering capabilities and weapons system-specific contests involves some artificiality. When a larger boundary is drawn to encompass all three US-Sino air-centric contests addressed in this study, different competitive standings may emerge. For instance, Chinese ballistic and cruise

missiles counter far more than just the US air defenses opposing them. Rather, they thwart US and allied attempts to stage air operations from locations near China.<sup>108</sup> Therefore, Chinese missiles represent part of the nation's competitive reaction to US fighters. As a corresponding counteraction, the DOD can choose to improve active and passive defenses of close fighter bases, to stage fighters from more distant locations enabled by greater numbers of tankers, or to employ some combination of these two actions. Even more indirectly, Chinese missiles may mitigate the US advantage in the fighter contest.

From a cost-imposition perspective, redrawing the cost boundary changes the accounting from just Chinese and US fighter costs to include Chinese ballistic and cruise missiles, US fighter base air defenses and US tanker and command-and-control costs required to project and coordinate fighters from sanctuary. Within this larger balance, the United States may have even less ability to create an advantageous hardship differential. When the contest considers these disparate but related capabilities, the DOD may find itself pushed further left on the competitive spectrum. In the end, this effect was part of Schelling's point. The more a cost-imposition calculus expands beyond suboptimization of a specific contest, the more hardship differential becomes less relevant than which nation has the best overall strategy.<sup>109</sup>

## **Conclusion**


While cost imposition retains its appeal, successful application of the strategy starts with recognizing what the approach is and what it is not. Cost imposition occupies one extreme of the cost-based competitive spectrum and offers advantageous hardship differential between an initiating competitor and a reacting opponent in a limited number of instances. Currently, these instances may be even more limited, given disproportionately high US defense investment relative to all competitors, including China. Cost imposition is not a stand-alone remedy for the DOD's fiscal constraints, but it has potential as a multiplier effect on the balances attained by expenditures within those constraints. The strategy will not bankrupt China, and it loses utility when used to lament or to justify the expense of defending US security interests. The DOD should develop some new organizational structures or adapt existing ones to implement long-term competition with rivals. The Competitive Strate-

gies Office approach of the 1980s was sufficient to the task then, and it most likely would be now.<sup>110</sup> The Joint Staff, service staffs, and combatant command staffs should accommodate the change, as each will play its part in conceiving, tailoring, executing, and adjusting the approach.

Successful cost-imposing strategies will require net assessments of the United States and each prospective rival and will place specific demands on US intelligence resources. To realize an advantageous hardship differential, the DOD will need an in-depth understanding of the Chinese economy, including all facets of the nation's military spending. Even then, the cost-imposition calculus will be somewhat artificial—bounded to be as inclusive as possible while still meaningful—and reliant on some type of exchange rate to better compare very different economies. Before making program, posture, and operating concept choices promising cost-imposing advantage, defense decision makers should ask hard questions about theories of interaction, reactions and counterreactions, and quantitative accounting. Theories of interaction only gain predictive utility when based on sufficient insights defining the adversary's decision calculus leading to primary and alternative reactions.

Managed competition between the United States and China in the military domain will require a mix of restraint and aggressiveness. The interdependencies of the two nations and potential collateral effects on third parties commend thoughtful, deliberate action. China's large competitive steps, begun in the mid-1990s to counter US capabilities, suggest that competitive and cost-imposing strategies have a high likelihood of eliciting significant reactions. The DOD should take a very long-term, calculated, and adaptive approach to the threats posed by Chinese ballistic and cruise missiles, SAM systems, and fighter aircraft. The ability to contest each of these Chinese capabilities falls at a different place on the competitive spectrum. For the security of the United States and to meet US responsibilities in other regions of the world, defense decision makers must do much better to optimize US performance within and among these competitions. The DOD should embark on cost-imposing initiatives fully cognizant of the expected and alternative outcomes, as informed by their underlying interaction theories and net assessment insights. By sharing the insights and assumptions informing a choice, defense decision makers can improve the likelihood that individual service supporting actions are coherent. The Office of Net Assessment, or a similar group, will have to conduct the deep and holistic understanding

of prospective competitors along with an inclusive appreciation of US attributes. Were the Office of the Secretary of Defense's program review process to include a cost-imposition facet, potential changes might be minor adjustments rather than major course corrections. However, cost-imposing strategies will frustrate the collective attention span of the DOD and may not survive the more self-interested, less spendthrift, Congressional review process.

The concept of cost imposition can yield new clarity when examining security alternatives for the services, the DOD, and the nation. It provides another attribute that, when considered in evaluating alternatives, can lead to better decisions that maximize competitive advantage. DOD-wide, cost-imposition principles can recast investment trade space, refocus regional presence and posture goals in a manner that rebalances near-term conflict preparedness with long-term competitive shaping, and provide new impetus for component interactions and the operating concepts they become. For the nation, cost imposition can provide a new framework for evaluating America's security challenges, which may suggest new options and priorities over current approaches. 

## Notes

1. Maj Gen Steven L. Kwast (director, US Air Force *Quadrennial Defense Review*), discussion with author, Washington, DC, 21 November 2013.
2. Stephen Waller, Col Case Cunningham, and Capt Keith Wheeler (Defense Advanced Research Projects Agency), interview by the author, 6 February 2014.
3. Gen Herbert J. Carlisle, "Viewing the Asia-Pacific Rebalance through the Lens of PACAF's Strategy" (address, Air Force Association Convention, Washington, DC, 18 September 2013).
4. Congressman Randy Forbes' official web site, "Amendment Offered by Mr. Forbes of Virginia: H. R. 4310 – National Defense Authorization Act for Fiscal Year 2013. Competitive Strategies Study," [http://forbes.house.gov/uploadedfiles/forbes\\_competitivestrategies.pdf](http://forbes.house.gov/uploadedfiles/forbes_competitivestrategies.pdf).
5. Caspar W. Weinberger, *Annual Report to the Congress: Fiscal Year 1988* (Washington, DC: Government Printing Office, 12 January 1987), 88.
6. Thomas C. Schelling, "The Strategy of Inflicting Costs," in *Issues in Defense Economics*, ed. Roland N. McKean (Cambridge, MA: National Bureau of Economic Research, 1967), 118–20.
7. International Law and Policy Institute Nuclear Weapons Project, "The Nuclear Umbrella States," Nutshell Paper No. 5 (Oslo, Norway: International Law and Policy Institute, 2012), 1–2.
8. Phillip C. Saunders and Joshua K. Wiseman, "China's Quest for Advanced Aviation Technologies," in *The Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard



P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: National Defense University [NDU] Press, 2012), 300–02.

9. Weinberger, *Annual Report to Congress*, 66.

10. Andrew W. Marshall, *Long-Term Competition with the Soviets: A Framework for Strategic Analysis* (U) (Santa Monica, CA: RAND Report R-862-PR, April 1972), iii.

11. David J. Andre, *Review of the Department of Defense (DOD) Competitive Strategies Initiative, 1986–1990*, vol. 1 (McLean, VA: SAIC Report SAIC 90/1506, 30 November 1990), 11–14.

12. Ibid., 66–69.

13. Ibid., 66.

14. Ibid.

15. Ibid.

16. Randall A. Greenwalt, David J. Andre, et al., *Historical Examples of Competitive Strategies* (Greenwood Village, CO: SAIC Report SAIC-91/ 6004&FSRC-E, 23 March 1991), 2.24.

17. Weinberger, *Annual Report to Congress*, 66. However, cost advantages attributed to the United States in this case may be overstated. The intensity of US investment required to develop, field, and sustain its bomber fleet does not draw much mention. To establish a true hardship differential in this area, more rigorous accounting is necessary. For example, initial procurement costs for the B-47, B-52, FB-111, B-1A and 1B, KC-135, KC-10, and B-2 were approximately \$128 billion in 1987 dollars. This sum excluded modernization investments plus substantial costs associated with personnel, installations, and operations. US Naval War College economist and former Deputy Assistant Secretary of Defense for Policy Planning Thomas Mahnken noted, “there has been no detailed case study of this interaction, particularly one incorporating Russian resources.” Thomas G. Mahnken, ed., *Competitive Strategies for the 21st Century: Theory, History, and Practice* (Stanford, CA: Stanford University Press, 2012), 302. Pending further substantiation, it may be correct to say that US cost imposition against the Soviets in the contest between penetrating bombers and air defenses was a qualified success. I derived the \$128 billion figure from initial procurement costs listed in *Selected Acquisition Reports*, or best available unit cost data for each aircraft applied to the inventory, inflated or deflated using consumer price index values to achieve 1987 values for comparison with Weinberger’s Soviet cost data.

18. Greenwalt, et al., *Historical Examples of Competitive Strategies*, 2.28. Advanced cruise missiles are mentioned more explicitly in Weinberger’s 1988 report to Congress.

19. Weinberger, *Annual Report to Congress*, 66. The 12,000-mile figure comes from Andrew F. Krepinevich, Simon Chin, and Todd Harrison, *Strategy in Austerity* (Washington, DC: Center for Strategic and Budgetary Assessments, 2012), xx.

20. Krepinevich, et al., *Strategy in Austerity*, xix.

21. Weinberger, *Annual Report to Congress*, 85.

22. Ibid., 69.

23. Dr. Thomas P. Ehrhard (Office of the Undersecretary of Defense for Policy), discussion with the author, 26 September 2013.

24. Michael Horowitz, *The Diffusion of Military Power Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010), 28.

25. Some weapons systems elude accounting by virtue of their classification. Special access programs vary in their degrees of acknowledgement and disclosure. “Black program” expenditures require separate accounting, making them more difficult to include in any cost-imposition calculus, despite the sizeable monetary investments some of these programs

represent. It is reasonable to assume that America's security competitors have weapon-systems programs shrouded in similar levels of secrecy. However, no accurate cost balance, much less capability comparison, can occur without factoring in classified programs for both sides. Temporal boundaries also affect the calculus. The obvious approach involves comparing investments in competing or countering systems and their associated enablers from the same point in time. However, nations do not necessarily field competing weapon systems concurrently. In the capability-improvement spiral associated with an arms race, one nation's investment in a system in time begets a rival's investment in a system of equal or greater capability. Using a fighter aircraft example, the greater capabilities and numbers of the Soviet MiG-23 and MiG-27 fielded in 1970 and 1975 prompted the United States to field the F-15 and F-16 in 1976 and 1978 respectively, which in turn led the Soviets to field the MiG-29 and Su-27 in 1983 and 1985 respectively. To determine the victor in this cost-imposition contest, which dates or weapons system introductions should be used in bounding the comparison?

26. The World Bank, "Military Expenditure (% of GDP)," Stockholm International Peace Research Institute, n.d., <http://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS>. The total expenditure of \$646 billion includes wartime costs and is cited in a variety of source to include, for consistency, James Steinberg and Michael E. O'Hanlon, *Strategic Reassurance and Resolve: U.S.-China Relations in the Twenty-First Century* (Princeton, NJ: Princeton University Press, 2014), 85.

27. Ibid. Steinberg and O'Hanlon address the wide variation of Chinese military expenditure estimates. I have used theirs for consistency. These authors (page 92) and the World Bank estimate Chinese defense spending at approximately 2 percent of GDP.

28. Steinberg and O'Hanlon, *Strategic Reassurance and Resolve*, 98.

29. Daniel I. Gouré, "Overview of Competitive Strategies Initiative," in *Competitive Strategies for the 21st Century: Theory, History, and Practice*, ed. Thomas G. Mahnken (Stanford, CA: Stanford University Press, 2012), 93.

30. Horowitz, *Diffusion of Military Power*, 1–5.

31. Schelling, "Strategy of Inflicting Costs," 109.

32. Ibid.

33. Ibid.

34. Ian Wallace (Brookings Institution), interview by the author, Washington, DC, 2 October 2013. While these were not his primary concerns, Wallace was the first person to highlight (to me) third-party considerations in a competitive interaction.

35. Samuel P. Huntington, "Arms Races: Prerequisites and Results," *Public Policy* 8, no. 41 (1958): 41–86.

36. Steinberg and O'Hanlon, *Strategic Reassurance and Resolve*, 4, 168, 173, 176, and more.

37. Ibid., 100–01.

38. Thomas G. Mahnken, Dan Blumenthal, Thomas Donnelly, Michael Mazza, Gary J. Schmitt, and Andrew Shearer, *Asia in the Balance: Transforming U.S. Military Strategy in Asia* (Washington, DC: American Enterprise Institute, June 2012), 9.

39. Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 113.

40. Ibid., 15.

41. Ibid., 203–16.

42. Owen R. Cote Jr., "Assessing the Undersea Balance between the United States and China," in *Competitive Strategies for the 21st Century: Theory, History, and Practice*, ed. Thomas G. Mahnken (Stanford, CA: Stanford Security Studies, 2012), 184–203.

43. Ibid., 184.
44. Ibid., 185–87.
45. Ibid., 185–86.
46. Ibid.
47. Horowitz, *Diffusion of Military Power*, 9.
48. Ibid., 98–133.
49. Ibid., 26–27.
50. Schelling, “Strategy of Inflicting Costs,” 114–18.
51. Ibid.
52. Thomas F. Lynch, III, *Crisis Stability and Nuclear Exchange Risks on the Subcontinent: Major Trends and the Iran Factor* (Washington, DC: NDU Press, 2013), 2–3. While not focused on the whole of conflict stability, this narrow discussion provided me with a better sense of the principles involved.
53. Glenn A. Kent, David A. Ochmanek, Michael Spirtas, and Bruce Pirnie, *Thinking about America’s Defense: An Analytical Memoir* (Santa Monica, CA: RAND, 2008), 141–43.
54. Nuclear Threat Initiative, “Treaty between the United States of America and the Union of Soviet Socialist Republics on Strategic Offensive Reductions (START II),” 3 January 1993, <http://www.nti.org/treaties-and-regimes/treaty-between-united-states-america-and-union-soviet-socialist-republics-strategic-offensive-reductions-start-ii>.
55. Michael O’Hanlon (Brookings Institution), interview by author, Washington, DC, 18 December 2013.
56. Ibid.
57. Sun Tzu, *Art of War*, trans. Ralph D. Sawyer (Boulder, CO: Westview Press, Inc., 1994), 215.
58. Steinberg and O’Hanlon, *Strategic Reassurance and Resolve*, 89.
59. Ibid., 93.
60. Ibid., 91.
61. James R. Holmes, “The State of the U.S.-China Competition,” in *Competitive Strategies for the 21st Century: Theory, History, and Practice*, ed. Thomas G. Mahnken (Stanford, CA: Stanford Security Studies, 2012), 135–36.
62. Mahnken, ed., *Competitive Strategies for the 21st Century*, 302.
63. US DOD, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: DOD, January 2012), 2; and Susan E. Rice, “America’s Future in Asia” (speech, Georgetown University, Washington, DC, 20 November 2013).
64. David Frelinger and Jessica Hart, “The U.S.-China Military Balance Seen in a Three-Game Framework,” in *The Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 347.
65. Ibid., 349.
66. Ibid., 351.
67. Ibid., 353.
68. Office of the Secretary of Defense (OSD), *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2013* (Washington, DC: OSD, 2013), 15.
69. Ibid.
70. Ibid., 29.

71. Xiaoming Zhang, "The PLAAF's Evolving Influence within the PLA and upon National Policy," in *Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 78–79.
72. Murray Scot Tanner, "The Missions of the People's Liberation Army Air Force," in *Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 136.
73. OSD, *Annual Report to Congress*, 15.
74. Zhang, "PLAAF's Evolving Influence," 72.
75. Kenneth W. Allen, "The Organizational Structure of the PLAAF," in *Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 95.
76. National Air & Space Intelligence Center, *People's Liberation Army Air Force 2010* (Wright-Patterson AFB, OH: NASIC Public Affairs, 2010), 16.
77. Zhang, "PLAAF's Evolving Influence," 74.
78. Kenneth Allen, *The Ten Pillars of the People's Liberation Army Air Force: An Assessment* (Washington, DC: Jamestown Foundation, April 2011), 6.
79. OSD, *Annual Report to Congress*, 5.
80. Hsi-hua Cheng, "The Employment of Airpower in the Taiwan Strait," in *The Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 330.
81. *Ibid.*, 339.
82. OSD, *Annual Report to Congress*, 5–6.
83. Joakim Kasper Oestergaard Balle, "About the THAAD System," *Aeroweb* (web site), 22 October 2014, <http://www.bga-aeroweb.com/Defense/THAAD.html>.
84. US Government Accountability Office, *Missile Defense: Opportunity to Refocus on Strengthening Acquisition Management*, GAO 13-432 (Washington, DC: Government Printing Office, April 2013), 33.
85. US DOD, *Quadrennial Defense Review* (Washington, DC: DOD, March 2014), 38.
86. Christopher J. Bowie, "The Lessons of Salty Demo," *Air Force Magazine*, March 2009, 55–57.
87. David Shlapak, "Equipping the PLAAF: The Long March to Modernity," in *The Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 206.
88. *Ibid.*
89. Alexey Eremenko, "5 Questions on Russian S-300 Missile System Sales to Syria," *RIA Novosti*, 14 May 2013, <http://en.ria.ru/analysis/20130514/181146715.html>.
90. William M. Ibinson, (analyst, Office of the Secretary of Defense, Cost Assessment, and Program Evaluation), discussion with the author, 9 January 2014.
91. Bill Sweetman, "Boeing, Lockheed Martin Form New Bomber Team," *Aviation Week and Space Technology*, 4 November 2013, [http://www.aviationweek.com/Article.aspx?id=/article-xml/AW\\_11\\_04\\_2013\\_p22-631732.xml](http://www.aviationweek.com/Article.aspx?id=/article-xml/AW_11_04_2013_p22-631732.xml).
92. Mark A. Stokes, "China's Quest for Joint Aerospace Power: Concepts and Future Aspirations," in *The Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 34; and OSD, *Annual Report to Congress*, 31.
93. Kevin Pollpeter, "The PLAAF and the Integration of Air and Space Power," in *The Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 174.



94. Roger Cliff, "The Development of the PLAAF's Doctrine," in *The Chinese Air Force: Evolving Concepts, Roles, and Capabilities*, ed. Richard P. Hallion, Roger Cliff, and Phillip C. Saunders (Washington, DC: NDU Press, 2012), 159.
95. Michael W. Pietrucha, "Frontier Basing: Making 'Places, Not Bases' A Reality," unpublished paper, version 2.0, 2013.
96. US Government Accountability Office, *F-35 Joint Strike Fighter: Restructuring Has Improved the Program, But Affordability Challenges and Other Risks Remain*, GAO 13-690T (Washington, DC: Government Printing Office, June 2013), 1.
97. Shlapak, "Equipping the PLAAF," 192.
98. Col Ralph J. Waite (analyst, Office of the Secretary of Defense, Cost Assessment, and Program Evaluation), discussions with the author, 18–20 February 2014. Based on *Selected Acquisition Reports*, 266 USAF fighter aircraft procured during this period consisted of 30 F-16s, 27 F-15Es, 184 F-22s, and 25 F-35As.
99. Lockheed Martin, "Lockheed Martin Celebrates 100th F-35 Lightning," 13 December 2013, [http://www.lockheedmartin.com/us/news/press-releases/2013/december/131213ae\\_lockheed-martin-celebrates-100th-f-35.html](http://www.lockheedmartin.com/us/news/press-releases/2013/december/131213ae_lockheed-martin-celebrates-100th-f-35.html).
100. James R. Fitzsimonds, "Cultural Barriers to Implementing a Competitive Strategy," in *Competitive Strategies for the 21st Century: Theory, History, and Practice*, ed. Thomas G. Mahnken (Stanford, CA: Stanford Security Studies, 2012), 290; and Allen, *Ten Pillars of PLAAF*, 5.
101. Robert Hewson, "Electric Dragons—Airborne Electronic Warfare Capabilities in China," *RUSI Defense Systems*, Spring 2012, 80.
102. Ibid.
103. Ibid., 81.
104. Saunders and Wiseman, "China's Quest for Advanced Technologies," 312.
105. Ibid., 302–03.
106. Allen, *Ten Pillars of PLAAF*, 37.
107. National Air & Space Intelligence Center, *People's Liberation Army Air Force 2010*, 15.
108. OSD, *Annual Report to Congress*, 32–33.
109. Schelling, "Strategy of Inflicting Costs," 109.
110. Andre, *Review of Competitive Strategies*, 117–20.

# Detering Malicious Behavior in Cyberspace

*Scott Jasper*

## Abstract

Recent incidents reveal cyberattacks are being employed and honed in a systematic, coordinated fashion to achieve the objectives of malicious actors. Deterrence of the wide array of actors in cyberspace is difficult, since deterrence has to work in the mind of the attacker. Each attacker will weigh the effort of the attack against the expected benefit under their own criteria or rationality. This article analyzes whether the contemporary and complementary deterrence strategies of retaliation, denial, and entanglement are sufficient to deter malicious cyber actors or if the alternative of active cyberdefense is necessary and viable.



Hackers, criminals, terrorists, foreign powers, and virtual states, a collection of actors working in concert online to influence world affairs, continue to probe and penetrate cyberspace.<sup>1</sup> Many of these actors seek our state secrets, trade secrets, technology, and ideas or aim to strike our critical infrastructure and to harm our economy.<sup>2</sup> Recent incidents reveal cyberattacks are being employed and honed in a systematic, coordinated fashion in an attempt to achieve competitors' objectives. In his first major television interview, the director of the Federal Bureau of Investigation, James Cook, said China has hacked every big US company looking for useful information; however, the cases investigated by the US Senate related to Chinese hackers breaking into computer networks of private transportation companies working for the US military

---

Scott Jasper, CAPT, USN, retired, is a lecturer at the Center for Civil-Military Relations and the National Security Affairs Department at the Naval Postgraduate School, specializing in defense capability development and cybersecurity. He is the editor of *Conflict and Cooperation in the Global Commons*, *Securing Freedom in the Global Commons*, and *Transforming Defense Capabilities: New Approaches for International Security*, and is a PhD candidate at the University of Reading, UK.

point more to preparing the digital battlefield for a potential conflict.<sup>3</sup> The Islamic State terrorist organization appears eager to enter into digital jihad, boasting of plans to establish a “cyber caliphate” from which to mount catastrophic hacking and virus attacks on the United States and the West.<sup>4</sup> Although their aspirations or objectives vary, the wide array of malicious actors in cyberspace has one thing in common: an expanding choice of cyberattack vectors to enact cyber aggression. Each attacker will weigh the effort of the attack against the expected benefit under their own criteria or rationality.

Given the ubiquitous nature of these threats, can malicious cyber actors be deterred? The aim of deterrence is to create disincentives for hostile action and normally involves two components: deterrence by punishment (the threat of retaliation) and deterrence by denial (the ability to prevent benefit). Some notable scholars have suggested a complementary third component: deterrence by entanglement (mutual interests) that encourages responsible behavior of actors based on economic and political relationships.<sup>5</sup> However, are contemporary and complementary deterrence strategies of retaliation, denial, and entanglement sufficient to dissuade and deter malicious cyber actors, or is an alternative required?

Deterrence of the wide array of actors in cyberspace is difficult, since deterrence has to work in the mind of the attacker. The point of deterrence is to add another consideration to the attacker’s calculus.<sup>6</sup> Deterrence instills a belief that a credible threat of unacceptable counteraction exists, that a contemplated action cannot succeed, or that the cost of action outweighs the perceived benefits. Complicated issues, like attribution, legality, liability, privacy, trust, and verification hamper conventional strategies and beg for an alternative ability to influence malicious behavior. The controversial concept of active cyberdefense (proactive actions), which relies on forensic intelligence and automated countermeasures, offers such an alternative and could limit exposure to threats.

Before considering each of the four strategies mentioned above, it is instructive to first consider aspects of cyberattack vectors along with current threat-actor strategies. The complexity and severity of acts of cyber aggression indicate that implementation of any strategy will require cooperation among all stakeholders in industry, government, and defense spheres. A proven method for national cooperation is the comprehensive approach used in international stabilization and reconstruction

operations as witnessed through the North Atlantic Treaty Organization (NATO).

## **Attack Vectors and Actor Strategies**

A cyberattack vector is a specific method or technique to access equipment, computers, or systems to deliver a hostile payload for a malicious outcome. These vectors range from social engineering attacks, Internet Protocol (IP) address spoofing, web malware attacks, Bluetooth eavesdropping, and other malicious code delivery means by physical manifestation (like thumb drives).<sup>7</sup> Cyberattack vectors have grown in number, complexity, and sophistication. Their expansive propagation enables unbridled acts of cyber aggression, like theft or exploitation of data, disruption or denial of access or service, and destructive action—including corruption, manipulation, and damage or the alteration of data. The technical properties of cyberattack vectors that prevent attribution allow actors to operate with near anonymity and impunity.

Criminal exploitation, military or industrial espionage, nationalist hacker protests, and infrastructure infiltration or sabotage are prominent in competitor operations and campaigns. A diverse array of cyberattack vectors are used to threaten the security of industrial, commercial, governmental, and military systems and devices. Not only has the volume of malicious code, known as malware, increased to 31 million new strains in 2013, but also the means of delivery have expanded to take advantage of human and technological weaknesses and modern-day platforms. The most sensational and publicized attack vectors are various types of intrusions by groups of attackers categorized as an advanced persistent threat (APT) and assaults by distributed denial of service (DDoS) methods. APT hacking is designed to covertly penetrate networks and systems to steal or alter information, manipulate data, or cause damage. A DDoS assault disrupts web site availability by overwhelming network equipment with volumetric attacks or consuming resources with application-centric attacks.<sup>8</sup>

The buying or renting of malicious code viruses, exploits of code vulnerabilities, botnets, and command-and-control servers provide an array of tools and services for motivated threat actors and states. The state-criminal nexus is evident, as cyber intruders who commit crimes and espionage use similar methods, for instance Remote Access Trojan tools



that capture and extract information, including Poison Ivy, Ghost, and PlugX.<sup>9</sup> For those actors willing to pay, professional hackers are for hire, including the Hidden Lynx group, which operates from China. Hidden Lynx professionals obtain specific information that could be used to gain competitive advantages at both corporate and nation-state levels.<sup>10</sup> They have been involved in several high-profile campaigns, including Operation Aurora—the obscure APT intrusions on Google and more than 30 other companies disclosed in 2010.<sup>11</sup>

A medium-sized Chinese APT group (about 50 members) ran the NetTraveler cyberespionage campaign. This malware infected more than 350 victims in 40 countries from 2005 through 2013.<sup>12</sup> The group stole more than 22 gigabytes of data found on 30 command-and-control servers.<sup>13</sup> The domains of interest they sought were space exploration, nanotechnology, energy production, nuclear power, lasers, medicine, and communications.<sup>14</sup> However, not all cyberespionage campaigns for hire originate from China. An Indian APT group, possibly a commercial security firm that has targeted entities and industries mainly in Pakistan since September 2010, runs Operation Hangover. Oddly rudimentary, the group uses publicly available tools and basic obfuscation methods while exploiting only known and fixed vulnerabilities.<sup>15</sup>

In late 2012, then Secretary of Defense Leon Panetta warned that the attacks on energy companies in the Persian Gulf and on banks in the United States mark a significant escalation of the cyber threat and renewed concerns over still more destructive scenarios.<sup>16</sup> Whether or not these incidents are representative of catastrophic results is debatable, since Saudi Aramco production systems were not breached and the longest interruption of the US banks was merely hours. However, preparations for conflict indicate we may already be in Phase Zero (“Shape”) of cyberwarfare campaigns as postulated in the notional six-phase model of joint and multinational operations described in US joint doctrine.<sup>17</sup> The head of US Cyber Command (USCYBERCOM) stated in Congressional testimony that China was responsible for the APT intrusion into RSA SecurID systems.<sup>18</sup> Moreover, in February 2013, the long-suspected role of the Chinese People’s Liberation Army (PLA) in systematic cyber espionage and data theft was confirmed by a US security firm that exposed APT1, believed to be a military unit under the PLA General Staff Department.<sup>19</sup> The Pentagon made further allegations against China in its 2013 annual report, alluding to the use of “computer net-

work exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors.”<sup>20</sup> This sort of state-sponsored espionage threatens military operations and readiness.<sup>21</sup>

The cost to the United States in intellectual property (product plans, research results, and customer lists) and confidential business information (trade secrets, exploration data, and negotiation strategies) theft amounts to billions of dollars annually.<sup>22</sup> In May 2014 the Department of Justice indicted five members of the Chinese military on charges of computer fraud, damaging a computer, aggravated identify theft, and economic espionage.<sup>23</sup> The conspirators, working for Unit 61398 in the vicinity of Shanghai, stole trade secrets useful to Chinese companies, including state-owned enterprises. For example, they hacked into SolarWorld computers to steal files about production capabilities and cost structure while the Oregon-based company was an active litigant in trade cases against Chinese solar manufacturers that had dumped products into US markets at prices below fair value.

The term cybered conflict could be an appropriate moniker to frame the complexity and ambiguity of struggle involving cyberspace, including hybrid warfare and insurgent campaigns.<sup>24</sup> Cybered conflict characterizes “old and new forms of conflict born of, enabled through, or dramatically altered by cyberspace.”<sup>25</sup> For instance, cyberattacks occurred on both sides over the weekend of Crimea’s vote to secede from Ukraine and join Russia in March 2014. Beginning Saturday evening, NATO’s main public web site, which carried a statement by the secretary general over the illegitimacy of the vote, worked intermittently. A hacker group called Cyber Berkut said the attack was carried out by “patriotic” Ukrainians angry over NATO interference; of note, *Berkut* refers to the feared riot squads of ousted pro-Russian Ukrainian president Victor Yanukovich.<sup>26</sup> On Sunday, a wave of 42 DDoS attacks hit Ukrainian government sites. The Monday after the vote, 132 separate DDoS blasts, most likely by OpRussia and Russian Cyber Command hackers who opposed annexation, slammed Russian sites.<sup>27</sup> Political conflicts have also spawned cyberattacks against Western news organizations, evidenced by the Syrian Electronic Army, a group of pro-regime hackers, compromising external web sites and social media accounts of the *New York Times*, the *Associated Press*, *CNN*, the *Huffington Post*, and *Forbes* to gain publicity for the embattled Syrian regime.<sup>28</sup>

## **Complementary Deterrence Strategies**

Deterrence seeks to shape another's perception of costs and benefits. Deterrence requires national resolve to commit resources, enhance cooperation, or use force when necessary. In July 2013 the US chairman of the Joint Chiefs of Staff, Gen Martin E. Dempsey, US Army, posited that national mission teams could counter threat actors' activities but recognized the need to work with other nations to set norms of responsible behavior in cyberspace, while improving information sharing and cyber standards.<sup>29</sup> In the Senate hearing to consider the nomination for the new commander of USCYBERCOM, Senator James Inhofe fittingly summarized the central problem in stating that "the lack of a cyber-deterrence policy . . . [has] left us more vulnerable to continued cyber aggression." When asked "how do we prevent that," the nominee, Vice ADM Michael S. Rogers, responded, "We're generating capability, we're generating capacity. . . . But in the end I believe we've got to get some idea of deterrence within the cyber arena."<sup>30</sup> The concept of deterrence is still hotly debated in the cyber community, because, for instance, traditional nuclear deterrence relies on an adversary having knowledge of the destruction that will result from transgressions, which is not possible in cyber because the secrecy of weapons is necessary to preserve their effectiveness.<sup>31</sup>

Deterrence stems from an adversary's belief that a threat of retaliation exists, that the intended action cannot succeed, or that the costs outweigh the benefits of acting.<sup>32</sup> The strategic debate during the Cold War over how best to deter nuclear attack normally was divided into deterrence by punishment (threat of retaliation) and deterrence by denial (limitation of damage).<sup>33</sup> Since today US policy would not condone the punishment of another country, a more appropriate view of this form of deterrence would simply be retaliation. With the strategic and economic interdependence that has resulted from contemporary globalization, one might also add deterrence by entanglement (mutual interests).<sup>34</sup>

For deterrence to be effective, it must be based on capability (possessing the means to influence behavior), credibility (instilling believability that counteractions may actually be deployed), and communication (sending the right message to the desired audience). The achievement of these conditions for effectiveness is extremely difficult. State capabilities to influence the behavior of threat actors in cyberspace are constrained by these actors' abilities to operate undiscovered for great lengths of

time; even if actors are convinced counteractions may be deployed, their rationality cannot be assumed. Additionally, the audience of actors conducting cyber aggression is vast and varied in motivations and intentions. No singularly sufficient answer exists to deter different types of groups using varied means of cyber aggression.

Identifying the need to “integrate newer behavioral approaches outside a rational state based actor construct,” the Assistant Chief of Staff for US Strategic Deterrence and Nuclear Integration, Maj Gen William A. Chambers, USAF, encourages moving beyond reliance solely on “imposition of costs to integrate denial of benefits and other methods for encouraging restraint.”<sup>35</sup> To make this move beyond Cold War-vestiges the focus must be on linking cyberdeterrence to desired effects, regardless of the actor being deterred.<sup>36</sup> The strategy of deterrence by entanglement can encourage responsible state behavior—to refrain from the conduct, endorsement, or allowance of malicious cyberactivity within a nation’s territory—through cooperation based on mutual interests. However, for the wider array of threat actors, a different paradigm or concept must be considered to achieve deterrence’s central premise—altering an adversary’s behavior. The concept of active cyberdefense that entails tenets of deterrence is another method for encouraging adversaries’ restraint. Automated, active cyberdefense-technologies can interdict, isolate, or remove threat vectors, denying benefit and engaging, deceiving, or stopping adversaries while imposing costs—regardless of the source.

US Department of Defense (DOD) cyberspace policy maintains effective deterrence is partly founded upon ensuring the capability to respond to hostile acts with a proportional and justified response.<sup>37</sup> This form of deterrence by retaliation is complicated by the difficulty in monitoring cyberspace, in identifying intrusions, and in locating the source with a high degree of confidence and in a timely manner. For example, advanced persistent threats conceal detection of attacker identities and allow plausible deniability. If definitive attribution can be obtained, the military could act within its prescribed authority in self-defense against an armed attack-equivalent in cyberspace. The cyberspace policy also recognizes effective deterrence in cyberspace is founded upon both the security and resilience of networks and systems. This strategy for deterrence discourages adversaries through the denial of benefit of their attack. In this context, security infers reducing risk by defensive cyber measures, and resilience means the ability to withstand and recover from



disruptions or attacks. Defensive measures emphasize the continual deployment of solutions to protect multiple threat points, including network, endpoint, web, and e-mail, from cyberattack vectors.

Pursuit of deterrence by entanglement through mutual interests has potential to reduce miscalculation and escalation. This strategy assumes potential adversaries are stakeholders in cyberspace, so embedded in the network they would not attack in peacetime or crisis. The deterrent effect is restraint based on the cost associated with attacks in cyberspace, in particular the loss of access for one's own purposes. Deterrence by entanglement involves encouraging others to accept a stake in the integrity of cyberspace through formal or informal rules or norms. The challenge in agreeing upon defined and achievable rules or norms that pertain to and are accepted by all state actors in the cyber realm lends credence to exploration of other options for achieving the effects of deterrence.

The DOD defines active cyberdefense as the synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities.<sup>38</sup> This definition implies the limitation of damage and elucidates the threat of retaliation—both elements of deterrence. Active cyberdefense is widely understood to include offensive actions in cyberspace taken for defensive purposes, with the limited goal of mitigating an immediate hostile act.<sup>39</sup> Federal or international laws and legislation govern any action beyond internal networks. Today “it’s illegal to chase bad guys up the wire, even if you have the capability to do so—it’s illegal to shoot back.”<sup>40</sup>

## **Deterrent Responses to Malicious Behavior**

Analyzing the sufficiency of deterrent responses—retaliation, denial, entanglement, or active defense—to influence malicious behavior by threat actors in cyberspace requires answering the following questions:

- Can threats of proportionate response realistically achieve deterrence by retaliation?
- Are defensive measures adequate to achieve deterrence by denial?
- Will cooperative measures restrain behavior through deterrence by entanglement?
- Is the concept of active cyberdefense technically and legally viable?

Feasible answers to these four questions are found in the following inspection of initiatives, issues, and constraints.

Deterrence by retaliation imposes costs for hostile acts in cyberspace. Retaliation is based on a nation's right to use all necessary means to defend itself, its allies and partners, and its interests in cyberspace. As appropriate and consistent with applicable international law, the means for a proportional and justified response includes diplomatic, informational, military, and economic measures.<sup>41</sup> Military response options may include using cyber- and/or kinetic capabilities. Under some circumstances, hostile acts in cyberspace could constitute an armed attack within the meaning of Article 51 of the United Nations (UN) Charter. Established principles would apply in the context of an armed attack (*jus ad bellum*). First, the right of self-defense applies against an imminent or actual armed attack whether the attacker is a state or nonstate actor. Second, the use of force in self-defense must be limited to what is necessary and proportionate to address an imminent or actual use of force. Third, states are required to take measures to ensure their territories are not used for purposes of armed activities against other states. Existing rules and principles of the international law of armed conflict address the use of cybertools in the context of armed conflict (*jus in bello*).

Regarding the question of whether or not a cyber operation constitutes an armed attack, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Rule 13) offers, that, it depends on the scale and effects.<sup>42</sup> Cyber operations that result in death or injury of individuals or destruction or damage of objects could rise to the level of an armed attack.<sup>43</sup> Although the Stuxnet computer worm caused physical damage, the International Group of Experts that developed the *Tallinn Manual* was divided on whether the damage constituted an armed attack. Future cyberattacks could be structured to transmit data or subtly modify, degrade, or corrupt data in a malicious but not immediately apparent manner.<sup>44</sup> NATO's Policy on Cyber Defense reiterates that any collective defense response is subject to political decisions by the North Atlantic Council.<sup>45</sup> This ambiguity gives an adversary good reason to use cyber as a method of attack against critical infrastructure.<sup>46</sup>

The imposition of costs in deterrence by retaliation is intended to reduce an adversary's willingness or ability to initiate or continue an offensive. While some argue the fundamental interconnectedness of networks means the effects of responsive cyber operations cannot be

limited, others claim that contained operations are possible even within broadly connected systems.<sup>47</sup> However, deliberate, inadvertent, or accidental escalation could trigger a chain reaction that raises the level of conflict beyond that contemplated by any party to the conflict.<sup>48</sup> In the United States, only the president can approve a cyber operation likely to result in significant consequences—a tough decision due to the inability to predict collateral damage and the uncertainty over political effect.<sup>49</sup> Equally, the threat of massive cyber retaliation would probably encourage actors to seek low levels of malicious behavior that fall below the threshold that would trigger such retaliation.<sup>50</sup> In many cases, target countries may be constrained to seek justice rather than retribution. In court, target states can press for access to individuals or to information and use refusal to cooperate as a justification for retaliation. However, until retaliation does ensue, there is no punishment—hence, no deterrence.<sup>51</sup> Meaning the threat alone of proportionate responses will not realistically achieve deterrence by retaliation.

Deterrence by denial of benefit denies an adversary's objectives by increasing the security and resilience of networks and systems. Traditional passive reactive methods, like antivirus software and blacklists, have grown ineffective as the volume and complexity of threats increase.<sup>52</sup> A defense-in-depth approach emphasizes the continual deployment of reactive solutions to protect multiple threat points, including network, endpoint, web, and e-mail security.<sup>53</sup> The spectrum of cybersecurity tools and techniques ranges from next-generation firewalls, application whitelisting, intrusion prevention systems and sandboxes to access control, data encryption, patch management, and data loss prevention. Layering multiple technologies combined with best practice endpoint management can decrease the risk of customized malware payloads, because each layer blocks a different aspect of multipronged cyberattacks. For example, at the delivery phase, device control can block infected Universal Serial Bus (USB) devices. At the exploitation phase, patch and configuration management can eliminate known vulnerabilities. At the installation phase, application control can prevent unapproved executables.<sup>54</sup> Cybersecurity frameworks suggest technical measures that can monitor networks and systems, detect attack attempts, identify compromised machines, and interrupt infiltration. The Council on Cyber Security's Critical Security Controls offers a prioritized program for computer security based on the combined knowledge of actual attacks

and effective defenses.<sup>55</sup> These controls cover a range of best practices, including vulnerability assessment, malware defenses, and access control. The controls identify commercial tools to detect, track, control, prevent, and correct weaknesses or misuse at threat points. The top three drivers for adopting these controls are increasing visibility of attacks, improving response, and reducing risk.<sup>56</sup> When the Congress failed to enact the necessary legislation, Pres. Barack Obama signed an executive order for the development of a Cybersecurity Framework that incorporates voluntary consensus standards and industry best practices. The inaugural Cybersecurity Framework is built around the core functions of identify, protect, detect, respond, and recover.<sup>57</sup> The Critical Security Controls are part of the Framework's informative references that illustrate methods to accomplish activities under these functions.

To facilitate cybersecurity information sharing, as called for in the executive order, the National Cybersecurity and Communications Integration Center (NCCIC) works with the private sector and government and international partners. The NCCIC strives to establish shared situational awareness of harmful activity, events, or incidents to improve the ability of partners to protect themselves. The NCCIC integrates analysis and data into a series of actionable and shareable information products. In addition, the NCCIC engages with information-sharing and analysis centers (ISAC) to protect portions of critical information technology with which they interact, operate, manage, or own. For example, during the 2012 series of DDoS assaults on US major banks, the NCCIC collaborated with the Financial Services ISAC to provide technical data and assistance to financial institutions. Data included DDoS-related IP addresses and supporting contextual information, which was also provided to over 120 international partners.<sup>58</sup>

Agencies and companies acknowledge the need to share more data about threats across enterprise boundaries but are worried about liability and risk. Commercial offerings, like Internet Identity's Active Trust platform, let contributors retain ownership of data and control dissemination.<sup>59</sup> However, only cybersecurity legislation can enable the private sector to share real-time cyber threat activity detected on its networks without fear of violating civil liberties and rights to privacy of citizens.<sup>60</sup> Thus, by design, participation in sharing arrangements and adoption of industry best practices for securing cyberspace remains voluntary for the private sector that largely owns the nation's critical infrastructure.<sup>61</sup>



Private sector awareness of threats, vulnerabilities, and consequences is questionable, when external parties reveal 85 percent of cyberespionage breaches months after intrusion.<sup>62</sup> Defensive measures are not adequate to achieve deterrence by denial, as security has not kept pace with the threat; more dynamic, active defenses are necessary. It is not a matter of if a company will be breached, but when. While the defense is not catatonic, it is not certain the offense will get continually better either, particularly when defense defines what the offense can do.<sup>63</sup>

Deterrence by entanglement encourages responsible behavior, while restraining malicious behavior through cooperation based on common interests. To some extent, nations share political, economic, commercial, and strategic dependency in cyberspace—as well as some degree of vulnerability. According to the UN secretary general, “While all Nations appreciate the enormous benefits of ICTs [information and communication technologies], there is also broad recognition that misuse poses risks to international peace and security.”<sup>64</sup> The secretary general’s report, authored by the Group of Governmental Experts, identifies that the development and spread of sophisticated tools and techniques increases the risk of mistaken attribution and unintended escalation. States have repeatedly affirmed the need for cooperative action against threats resulting from this malicious use. States must lead these efforts, but effective cooperation would benefit from participation by the private sector and civil society in a comprehensive approach. An array of actions is required to promote a peaceful, secure, and open information and communications technology environment.<sup>65</sup>

One action to strengthen deterrence by entanglement could be the implementation of formal binding agreements. Arms control aims to establish legal regimes that make conflict less likely. The objective of such regimes is to reduce the existence of, or restrict the use of, certain weapons. However, imposing limitations on the development and proliferation of cyberweapons is difficult, because their properties are incompatible with the rationale for arms-control treaties.<sup>66</sup> The lack of universal consensus on what even constitutes a cyberweapon complicates verification of compliance. Most of the technology relied on in an offensive capacity is inherently dual-use, like vulnerability assessment tools, and software can be minimally repurposed for malicious action.<sup>67</sup> Control of cyberweapon development, spread, and use is practically impossible. Cyberweapons require no controlled materials, identifiable manufactur-

ing facilities, or restricted skills.<sup>68</sup> Open-source software that could be used as a cyberweapon is widely available for free or for purchase, i.e., the Blackhole exploit kit.<sup>69</sup> Alternative devices and systems are continually being compromised and turned into cyberweapon platforms. Additionally, the creator or source of the weapon is not often the user, i.e., in hacktivist campaigns cybertools with instructions are provided to patriotic or ideological hackers supporting a cause.

Absent practical and acceptable treaties, cooperative measures could enhance international peace, stability, and security. Internationally acceptable norms, rules, and principles of responsible behavior by states could encourage order in the domain. These measures start with the premise that international law—in particular the Charter of the United Nations—is applicable to cyberspace. The Seoul Conference on Cyberspace resulted in a “Framework for and Commitment to Open and Secure Cyberspace” that offers guidelines for governments and organizations on coping with cybercrime and cyberwar.<sup>70</sup> These guidelines include verbatim recommendations by the UN Group of Government Experts for states to meet their international obligations regarding wrongful acts attributed to them, to refrain from using proxies to commit wrongful acts, and to ensure their territories are not used by nonstate actors for unlawful acts.

Regional or bilateral dialogue can establish voluntary confidence-building measures to promote trust and assurance, like those agreed upon by the United States and Russia for sharing of threat indicators.<sup>71</sup> Other practical measures to increase predictability and reduce misperception include exchange of views on national policies, like a recent briefing by the DOD given to Chinese officials regarding Pentagon doctrine for defending against cyberattacks.<sup>72</sup> Finally, capacity-building assistance might be necessary for states to fulfill their responsibilities for cyberspace. Efforts for assistance range from developing technical skill and sharing best practices to strengthening national legal frameworks. Overall, cooperative measures—international norms, confidence-building measures, and capacity-building assistance—are well-suited mechanisms for deterrence by entanglement. These mechanisms can address potential threats, vulnerabilities, and risks, but a clash of self-interests might thwart cooperation that restrains malicious behavior. For example, Beijing suspended a US-Sino working group on cyber-related issues after the indictment of the Unit 61398 members, citing “we should encourage

organizations and individuals whose rights have been infringed to stand up and sue Washington.”<sup>73</sup>

Active cyberdefense is defined as the “proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network.”<sup>74</sup> These tasks imply defensive measures and proportionate responses that shape an adversary’s perception of benefits and costs—the essence of deterrence. In military terms, the tasks are very similar to defensive cyberspace operations described by the director of operations at USCYBERCOM as “passive and active cyberspace defense activities that allow us to outmaneuver an adversary.”<sup>75</sup> Defensive cyberspace operations provide the ability to discover, detect, analyze, and mitigate threats with malicious capability and intent to affect key cyber terrain. Subcategories of these operations are internal defensive measures (IDM), actions taken internally, and response actions (RA) taken outside the information environment. Tasks for IDM are hunting on friendly terrain for threats and directing appropriate internal responses, whereas RA are about going after the shooter outside friendly network space to stop the attack.

For the private sector, active cyberdefense entails working with cybersecurity solution providers to identify and interdict cyber intrusions.<sup>76</sup> Once packets are determined to be malware, defensive actions can be taken, including diverting packets to a holding area or other actions aimed at the attacker. The broad spectrum of actions available include using honeypots, beaconing, sinkholing, and deceiving, which raise adversary costs and risks through interference, delay, obstruction, or trickery.<sup>77</sup> Even limited action would contribute to assurance (detection of intrusions) and attribution (identification of actors). Many public debates center on aggressive response aspects of active cyberdefense, like hack back, for which existing legal constraints would have to be adapted to allow use of these tactics.<sup>78</sup>

A more practical description of active cyberdefense is a range of proactive actions that engage the adversary before and during a cyber incident. Examples would be using a honeypot to see which documents the adversary chooses to exfiltrate, remotely tracking stolen documents by passive watermarks on files, or allowing the adversary to steal documents that contain false or misleading information.<sup>79</sup> Legal issues confront employing actions outside of the victim’s network, like taking control of

remote computers to stop attacks or launching denial of service attacks against attacking machines. The primary law in the United States that applies to these more aggressive techniques is the Computer Fraud and Abuse Act (CFAA), codified as Title 18, Section 1030. A defendant can violate the CFAA by accessing a “protected computer” without authorization or by exceeding authorized access.<sup>80</sup>

One could argue US common law admits certain rights of self-defense and of defense of property in preventing the commission of a crime against an individual or a corporation. Applying the latter for hostile cyberattacks, the range of allowable actions is roughly comparable to the range for *nonlethal* self-defense. While individuals are not permitted to engage in revenge or retaliation for a crime, they are—in some instances—entitled to take otherwise-prohibited actions for the purpose of preventing or averting an imminent crime or addressing one that is in progress. However, in most cases, challenges in quickly obtaining definitive attribution preclude exercising this right.<sup>81</sup> Therefore, under current law, a private-sector actor may realistically only respond to hostile attacks within its own networks and systems organizational boundaries. Only one active defense capability, HawkEye G, exists internal to the network today. It uses automated countermeasures to remove cyber threats before they can compromise intellectual property or cause process disruption.<sup>82</sup> Until legally viable for vendors to provide solutions outside the network, the concept is technically limited to denial of benefit.

## A Comprehensive Approach

The US Joint Staff recognizes the government and the private sector must plan and coordinate their activities to prepare for cyber threats. However, the staff also realizes that achieving unity of effort to meet national security goals is always problematic due to challenges in information sharing, competing priorities, and uncoordinated activities. Success in preparation and response to cyberattacks is dependent upon unity of effort enabled by collaboration and coordination among partners.<sup>83</sup> The US *Cyberspace Policy Review* also delineates the need for a comprehensive framework to facilitate coordinated responses by government, the private sector, and allies to a significant cyber threat or incident. The review maintains that “addressing network security issues requires a public-private partnership as well as international coopera-



tion and norms.”<sup>84</sup> Deterrence, as an element of cybersecurity policy, provides a strategic response that is underpinned by this partnership and cooperation. The challenge is to align the efforts of all involved parties for a common purpose. NATO has used the concept of a comprehensive approach to align parties in NATO operations by capitalizing on shared interests, complementary opportunities, and mutual procedures. The comprehensive approach is based on “principles and collaborative processes that enhance the likelihood of favorable and enduring outcomes within a particular situation.”<sup>85</sup> NATO proclaims “the need to promote a comprehensive approach applies not only to operations, but more broadly to many of NATO’s efforts to deal with 21st century security challenges, such as . . . protecting against cyber attacks.”<sup>86</sup>

Although NATO experiences offer a starting point to design a comprehensive approach for operations in a particular domain of interest (cyberdeterrence), the methodology must be modified and translated for different operational conditions, structural characteristics, and prominent partners, including commercial actors. The Comprehensive National Cybersecurity Initiative aims to build an approach to cyberdefense strategy that deters interference and attack in cyberspace. The White House provides a shining example of embracing a comprehensive approach for cyberdeterrence by suggesting public- and private-sector partnerships for cyberdefense of critical infrastructure sectors.<sup>87</sup> Within this context of a comprehensive approach, a partnership would be defined as close cooperation between parties having common interests in achieving a shared vision.

Given cooperative interaction can potentially facilitate the common interests of organizations, the comprehensive approach aims for congruence of purpose—not unity of command.<sup>88</sup> However, the approach needs to recognize and overcome a clash of self-interests—where one party strives to maintain economic or military advantage—that might prevent cooperation in deterring cyber aggression. For instance, the private sector is reluctant to share cyber threat data with the government, because it does not believe the latter can protect the confidentiality of a company that has been attacked, which may devalue stocks or compromise proprietary information to the advantage of competitors.<sup>89</sup> A state might not agree to cooperative action if binding rules constrain its preferred method of competition in cyberspace. Critical to gaining consensus for the comprehensive approach is the multilateral characteristic

of diffuse reciprocity, whereby parties recognize their self-interests will be satisfied over the long term. Examination of models and precedents in other functions or domains, like the emerging International Code of Conduct for Outer Space Activities, could identify principles, measures, and mechanisms that not only foster trust and cooperation but also facilitate openness and transparency.<sup>90</sup>

In reality, many cyber incidents today are merely easily-corrected annoyances—causing irritation, inconvenience, and perhaps delay.<sup>91</sup> Even the vaulted Stuxnet worm that resulted in the replacement of about 1,000 IR-1 centrifuges at the Iranian nuclear facility in Natanz, only exposed vulnerabilities in Iranian enrichment facilities that ultimately improved centrifuge performance.<sup>92</sup> Whether cyber means are capable of inflicting real persistent harm on the fighting power of an enemy is doubtful.<sup>93</sup> Likewise, the analytical basis for cyber alarmism is dubious, despite public policy makers ranting repeatedly about wake-up calls following cybersecurity incidents.<sup>94</sup> However, bolstering that stream of concern, the US Director of National Intelligence has testified, “We assess that the likelihood of a destructive attack that deletes information or renders systems inoperable will increase as malware and attack tradecraft proliferate.”<sup>95</sup> Admiral Rogers believes China, along with one or two other countries, already has cyber capabilities that could shut down the electric grid in parts of the United States.<sup>96</sup> A comprehensive approach has produced interaction among diverse organizations, leading to a more effective overall effort in operations.<sup>97</sup> For cyberspace, the framework could enable the implementation of complementary deterrence strategies or an alternative that achieves similar desired effects.

## Conclusion

The US chairman of the Joint Chiefs of Staff claims “disruptive and destructive cyber attacks are becoming a part of conflict,” and “civilian infrastructure and business are targeted first.”<sup>98</sup> In response, the *Quadrennial Defense Review* reiterates that deterrence of these sorts of cyber threats requires a multistakeholder coalition that enables “the lawful application of the authorities, responsibilities, and capabilities resident across the U.S. Government, industry, and international allies and partners.”<sup>99</sup> This mandate effectively endorses the use of a comprehensive approach to influence malicious behavior in cyberspace. The challenge

remains in the number and type of malicious actors with various motivations and the assortment of cyberattack vectors at their disposal. When asked whether the cyber intrusions on JP Morgan Chase, and at least four other banks, were coming from entities associated with the Russian government, US Secretary of the Treasury Jack Lew replied, "We have a lot of concerns about the sources of attacks because there are many different sources."<sup>100</sup>

The cyber breach at JP Morgan Chase Bank offers an illustrative case to examine the sufficiency of the suggested deterrence strategies or alternative. In June 2014, hackers used a phishing attack vector to compromise a bank employee's user name and password and enter a web-development server. With a variety of malware, the hackers eventually gained access to more than 100 servers that housed personal data, but not account information, for 76 million household accounts.<sup>101</sup> Many believe the attacks were a direct result of sanctions imposed by the United States against Russia. The lack of any apparent profit motive generates speculation that the hackers were sponsored by the Russian government. For this case, deterrence by retaliation, by at least military means, falters as the incident does not cross any threshold for an armed attack. For deterrence by denial, JP Morgan's chairman admits that even though the bank has fortified its defenses (with a \$250 million annual digital security budget) the battle is "continual and likely never-ending."<sup>102</sup> For deterrence by entanglement, the question is, would the Russian government investigate if asked, especially if the attack was indeed conducted by a proxy group on their behalf. Additionally, for the active cyberdefense concept, while the initial authenticated entry would not have been blocked, the breach might have been detected earlier by capabilities that discover and interpret subtle behaviors in enterprise activity.

In not only the above suspected case of state-sponsored espionage but also in other disruptive or destructive forms of cyber aggression, each suggested deterrence strategy has limited merit in preventing threat-actor action. The promise of active cyberdefense is in autonomous countermeasures that act without regard to the identity of the malicious threat actors or their motivations—only that their malware is isolated or eradicated. Although active defense can close the time between discovery and compromise, many organizations are reluctant to adopt machine-enabled defenses for fear of algorithmic misfires with unexpected consequences. Despite preventive efforts, attacks continue

and increase in sophistication. Malicious actors are using multiple-stage attacks, stretched out over months or using new infection vectors.<sup>103</sup>

The proliferation of threat vectors and actors will not allow pause for policy makers to get some idea of deterrence within the cyber arena. Deterrence convinces adversaries not to take malicious actions by means of decisive influence over their decision making. Decisive influence is achieved by threatening to impose costs or deny benefits while imposing restraint.<sup>104</sup> The solution to the dilemma is a mix of strategies and capabilities that influence the decision-making process of an actor, regardless if rational or not. Ways do exist to enhance the sufficiency of the suggested responses, including imposing real consequences (retaliation), employing reactive defenses (denial), sustaining diplomatic perseverance (entanglement), and considering legal adaptation (active defense). The suggested responses are at least a starting point to achieving an end state where the actor chooses not to act for fear of some combination of cost, failure, or consequences. **SSQ**

## Notes

1. Kevin G. Coleman, "Virtual States in Cyberspace Increase in Size and Numbers," *DefenseSystems.com*, 15 November 2012, <http://defensesystems.com/articles/2012/11/15/digital-conflict-virtual-states.aspx>.

2. Robert Anderson Jr., *Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland; Testimony before the Committee on Homeland Security and Government Affairs, United States Senate*, 113th Cong., 2nd sess., 10 September 2014, <http://www.hsgac.senate.gov/download/?id=36272b88-c26a-45d8-887e-814fc8c8eb04>.

3. James Cook, "FBI Director: China Has Hacked Every Big US Company," *Business Insider*, 6 October 2014, <http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10>; and Danny Yadron, "Chinese Hacked U.S. Military Contractors, Senate Panel Says Hackers Broke into Computer Networks 20 Times in a Year," *Wall Street Journal*, 18 September 2014, <http://online.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says-1410968094>.

4. Jamie Dettmer, "Digital Jihad: ISIS, Al Qaeda Seek a Cyber Caliphate to Launch Attacks on US," *FoxNews.com*, 14 September 2014, <http://www.foxnews.com/world/2014/09/14/digital-jihad-isis-al-qaeda-seek-cyber-caliphate-to-launch-attacks-on-us/>.

5. Schuyler Foerster, "Strategies of Deterrence," in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, ed. Scott Jasper (Washington, DC: Georgetown University Press, 2012), 64.

6. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 6–37, [http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND\\_MG877.pdf](http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf).

7. Kevin G. Coleman, *The Cyber Commander's eHandbook: The Strategies and Tactics of Digital Conflict*, version 4 (McMurray, PA: Technolytics, 2013), 52–80.



8. Chris Pepper, ed., *Defending against Denial of Service Attacks* (Phoenix, AZ: Securosis, 31 October 2012), 1–24, [https://securosis.com/assets/library/reports/Securosis\\_Defending-Against-DoS\\_FINAL.pdf](https://securosis.com/assets/library/reports/Securosis_Defending-Against-DoS_FINAL.pdf).

9. Kelly Jackson Higgins, “Chinese Cyberespionage Tool Updated for Traditional Cybercrime,” *Dark Reading*, 27 November 2012, <http://www.darkreading.com/attacks-breaches/chinese-cyberespionage-tool-updated-for-traditional-cybercrime/d/d-id/1138733?>.

10. Stephen Doherty, Jozsef Gegeny, Branko Spasojevic, and Jonell Baltazar, *Hidden Lynx—Professional Hackers for Hire*, version 1.0 (Mountain View, CA: Symantec, 17 September 2013), [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/hidden\\_lynx.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf).

11. William Jackson, “How Google Attacks Changed the Security Game,” *Government Computer News*, 1 September 2010, <http://gcn.com/articles/2010/09/06/interview-george-kurtz-mcafee-google-attacks.aspx?m=1>.

12. Kaspersky Lab’s Global Research and Analysis Team, *The NetTraveler (aka Travnet)* (Moscow, Russia: Kaspersky Lab, 2013), 1–25, <http://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/kaspersky-the-net-traveler-part1-final.pdf>.

13. Kelly Jackson Higgins, “‘NetTraveler’ Cyberespionage Campaign Uncovered,” *Dark Reading*, 4 June 2013, <http://www.darkreading.com/attacks-breaches/nettraveler-cyberespionage-campaign-uncovered/d/d-id/1139884?>.

14. Kaspersky Lab’s Global Research and Analysis Team, “NetTraveler Is Running! Red Star APT Attacks Compromise High-Profile Victims,” *Securelist*, 4 June 2013, <http://securelist.com/blog/research/35936/nettraveler-is-running-red-star-apt-attacks-compromise-high-profile-victims/>.

15. Kelly Jackson Higgins, “‘Commercialized’ Cyberespionage Attacks Out of India Targeting U.S., Pakistan, China, and Others,” *Dark Reading*, 20 May 2013, <http://www.darkreading.com/attacks-breaches/commercialized-cyberespionage-attacks-out-of-india-targeting-us-pakistan-china-and-others/d/d-id/1139791?>.

16. Leon E. Panetta, “Defending the Nation from Cyber Attack” (speech, Business Executives for National Security, New York, 11 October 2012), <http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1728>.

17. US Joint Publication 5-0, *Joint Operation Planning*, 11 August 2011, III-38–III-44.

18. Kelly Jackson Higgins, “China Hacked RSA, U.S. Official Says,” *Dark Reading*, 29 March 2012, <http://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409?>.

19. Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units* (Alexandria, VA: Mandiant, 27 February 2013), [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf).

20. Office of the Secretary of Defense (OSD), *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China* (Washington, DC: DOD, May 2013), 36, [http://www.defense.gov/pubs/2013\\_china\\_report\\_final.pdf](http://www.defense.gov/pubs/2013_china_report_final.pdf).

21. Larry M. Wortzel, *Cyber Espionage and the Theft of US Intellectual Property and Technology: Testimony before the Committee on Energy and Commerce, US House of Representatives*, 113th Cong., 1st sess., 9 July 2013, <http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-Wortzell-20130709-U1.pdf>.

22. James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, July 2013), [http://csis.org/files/publication/60396rpt\\_cybercrime-cost\\_0713\\_ph4\\_0.pdf](http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf).

23. *United States of America v. Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, Gu Chunhui*, in United States District Court for the Western District of Pennsylvania, indictment, Criminal No. 14-118, filed 1 May 2014, 1–48.

24. Chris Demchak, “Cybered Conflict, Cyber Power, and Security Resilience as Strategy,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 121–36.

25. Peter Dombrowski and Chris Demchak, “Cyber War, Cybered Conflict, and the Maritime Domain,” *Naval War College Review* 67, no. 2 (Spring 2014), 3, <https://www.usnwc.edu/getattachment/762be9d8-8bd1-4aaf-8e2f-c0d9574afec8/Cyber-War,-Cybered-Conflict,-and-the-Maritime-Doma.aspx>.

26. Adrian Croft and Peter Apps, “NATO Websites Hit in Cyber Attack Linked to Crimea Tension,” *Reuters*, 16 March 2014, <http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316>.

27. Mark Clayton, “Massive Cyberattacks Slam Official Sites in Russia, Ukraine,” *Christian Science Monitor*, 18 March 2014, <http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0318/Massive-cyberattacks-slam-official-sites-in-Russia-Ukraine>; and Jeffrey Carr, “Rival Hackers Fighting Proxy War over Crimea,” *CNN Opinion*, 25 March 2014, <http://www.cnn.com/2014/03/25/opinion/crimea-cyber-war/>.

28. Mandiant, *M Trends: Beyond the Breach* (Alexandria, VA: Mandiant, April 2014), 1–7, [https://dl.mandiant.com/EE/library/WP\\_M-Trends2014\\_140409.pdf](https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf); and Patrick Tucker, “Syrian Electronic Army Threatens to Hack CENTCOM,” *Defense One*, 3 March 2014, <http://www.defenseone.com/technology/2014/03/syrian-electronic-army-threatens-hack-centcom/79777/>.

29. Martin E. Dempsey, “Defending the Nation at Network Speed” (discussion, Brookings Institution, 27 June 2013), <http://www.brookings.edu/events/2013/06/27-defense-cyber-security-dempsey>.

30. *Hearing to Consider the Nominations of: Gen Paul J. Selva, USAF, for Reappointment to the Grade of General and to be Commander, US Transportation Command; and VADM Michael S. Rogers, USN, to be Admiral and Director, National Security Agency/Chief, Central Security Services/Commander, US Cyber Command; Statements Before the Senate Committee on Armed Services*, US Senate, 113th Cong., 2nd sess., 11 March 2014, <http://www.armed-services.senate.gov/imo/media/doc/14-16%20-%203-11-14.pdf>.

31. Zachary Fryer-Biggs, “US Cyber Moves beyond Protection,” *Defense News*, 16 March 2014, <http://www.defensenews.com/article/20140316/DEFREG02/303170013/US-Cyber-Moves-Beyond-Protection>.

32. Joint Publication 3-0, *Joint Operations*, 11 August 2011, V-10 and V-39.

33. Schuyler Foerster, “Theoretical Foundations: Deterrence in the Nuclear Age,” in *American Defense Policy*, 6th ed., ed. Schuyler Foerster and Edward Wright (Baltimore, MD: Johns Hopkins University Press, 1990), 47–51.

34. Roger G. Harrison, Deron R. Jackson, and Collins G. Shackelford, “Space Deterrence: The Delicate Balance of Risk,” *Space and Defense* 3, no. 1 (Summer 2009): 1–30.

35. William A. Chambers, “Foreword,” in *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, ed. Adam Lowther (Maxwell AFB, AL: Air University Press, 2014), xii.

36. Adam Lowther, “The Evolution of Deterrence,” in *Thinking about Deterrence: Enduring Questions in a Time of Rising Powers, Rogue Regimes, and Terrorism*, ed. Adam Lowther (Maxwell AFB, AL: Air University Press, 2014), 3–4.

37. DOD, *Department of Defense Cyberspace Policy Report* (Washington, DC: DOD, November 2011), 7, [http://www.defense.gov/home/features/2011/0411\\_cyberstrategy/docs/NDAA%20Section%20934%20Report\\_For%20webpage.pdf](http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf).

38. DOD, *Department of Defense Strategy for Operating in Cyberspace*, July 2011, 13, <http://www.defense.gov/news/d20110714cyber.pdf>.

39. Herbert S. Lin, "Defining Self-Defense for the Private Sector in Cyberspace," *World Politics Review*, 6 February 2013, 2, <http://www.worldpoliticsreview.com/articles/12694/defining-self-defense-for-the-private-sector-in-cyberspace>.

40. Patience Wait, "Cyberthreats Grow More Ominous: Former NSA Chief," *Information Week*, 11 October 2013, <http://www.darkreading.com/risk-management/cyberthreats-grow-more-ominous-former-nsa-chief/d/d-id/1111912?>.

41. Executive Office of the President, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (Washington, DC: The White House, May 2011), 13–14, [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf).

42. Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, May 2013), 54–61.

43. Michael N. Schmitt, "Attack as a Term of Art in International Law: The Cyber Operations Context," in *4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 283–93.

44. Martin R. Stytz and Sheila B. Banks, "Toward Attaining Cyber Dominance," *Strategic Studies Quarterly* 8, no. 1 (Spring 2014), 60, [http://www.au.af.mil/au/ssq/digital/pdf/spring\\_2014/stytz.pdf](http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/stytz.pdf).

45. North Atlantic Treaty Organization (NATO), "Defending the Networks: The NATO Policy on Cyber Defence" (policy statement, NATO, Brussels, Belgium, 8 June 2011).

46. Vincent Joubert, "Five Years after Estonia's Cyber Attacks: Lessons Learned for NATO?" (research paper 76, NATO Defense College, Rome, Italy, 2012), 5, [http://www.ndc.nato.int/news/current\\_news.php?icode=394](http://www.ndc.nato.int/news/current_news.php?icode=394).

47. Maren Leed, *Offensive Cyber Capabilities at the Operational Level* (Washington, DC: Center for Strategic & International Studies, September 2013), 2–3, [http://csis.org/files/publication/130916\\_Leed\\_OffensiveCyberCapabilities\\_Web.pdf](http://csis.org/files/publication/130916_Leed_OffensiveCyberCapabilities_Web.pdf).

48. Herbert Lin, "Escalation Dynamics and Conflict Termination in Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012), 52–55, <http://www.au.af.mil/au/ssq/2012/fall/lin.pdf>.

49. James Andrew Lewis, "Truly Damaging Cyberattacks Are Rare," *Washington Post*, 10 October 2013, [http://www.washingtonpost.com/postlive/truly-damaging-cyberattacks-are-rare/2013/10/09/ae628656-2d00-11e3-b139-029811dbb57f\\_story.html](http://www.washingtonpost.com/postlive/truly-damaging-cyberattacks-are-rare/2013/10/09/ae628656-2d00-11e3-b139-029811dbb57f_story.html).

50. Sean Lawson, "Putting the War in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States," *First Monday* 17, no. 7 (2 July 2012), <http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270>.

51. Martin Libicki, "Pulling Punches in Cyberspace," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (Washington, DC: National Academies Press, 2010), 123–47.

52. Lumension, *Redefining Defense-in-Depth* (Scottsdale, AZ: Lumension, March 2014), 1–6, [https://www.lumension.com/Media\\_Files/Documents/Marketing---Sales/Whitepapers/Redefining-Defense-in-Depth.aspx](https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Whitepapers/Redefining-Defense-in-Depth.aspx).

53. Ed Metcalf, *Counter Stealth Malware* (Santa Clara, CA: McAfee, 2013), 1–3, <http://www.mcafee.com/us/resources/solution-briefs/sb-counter-stealth-malware.pdf>.

54. Lumension, *Preventing Weaponized Malware Payloads in Advanced Persistent Threats* (Scottsdale, AZ: Lumension, February 2013), 1–4, [https://www.lumension.com/Media\\_Files/Documents/Marketing---Sales/Whitepapers/Lumension\\_2013-Feb1\\_wp\\_Preventing\\_Weaponized\\_Malwa.aspx](https://www.lumension.com/Media_Files/Documents/Marketing---Sales/Whitepapers/Lumension_2013-Feb1_wp_Preventing_Weaponized_Malwa.aspx).

55. Council on CyberSecurity, *Critical Controls for Effective Cyber Defense*, version 4.1 (Bethesda, MD: SANS [SysAdmin, Audit, Networking, and Security], Institute, March 2013), <https://ccsfiles.blob.core.windows.net/web-site/file/81d5ad9c89d242a7a555658e604fdc43/Critical%20Controls%20v4.1.pdf>.

56. John Pescatore and Tony Sager, *Critical Security Controls Survey: Moving from Awareness to Action*, SANS white paper (Bethesda, MD: SANS Institute, June 2013), [https://www.sans.org/media/critical-security-controls/CSC\\_Survey\\_2013.pdf](https://www.sans.org/media/critical-security-controls/CSC_Survey_2013.pdf).

57. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, version 1.0 (Washington, DC: NIST, 12 February 2014), <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>.

58. Roberta Stempfley and Lawrence Zelvin, *Facilitating Cyber Threat Information Sharing and Partnering with the Private Sector to Protect Critical Infrastructure: An Assessment of DHS Capabilities; Hearing before the House Committee on Homeland Security, US House of Representatives*, 113th Cong., 1st sess., 16 May 2013, <http://www.gpo.gov/fdsys/pkg/CHRG-113hhrg85613/html/CHRG-113hhrg85613.htm>.

59. William Jackson, “Social Platform for Sharing Cyberthreat Intell Goes Live,” *Government Computer News*, 11 February 2014, 6, <http://gcn.com/articles/2014/02/11/activetrust.aspx>.

60. Keith B. Alexander, *Statement of Gen Keith B. Alexander Commander US Cyber Command before the House Committee on Armed Services Subcommittee on Intelligence, Emerging Threats and Capabilities, US House of Representatives*, 113th Cong., 2nd sess., 12 March 2014, <http://docs.house.gov/meetings/AS/AS26/20140312/101883/HHRG-113-AS26-Wstate-AlexanderUSAK-20140312.pdf>.

61. Department of Homeland Security (DHS), *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: DHS, March 2013), 1–14, [http://www.dhs.gov/sites/default/files/publications/NIPP%202013\\_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience\\_508\\_0.pdf](http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf).

62. Verizon, *2014 Data Breach Investigations Report* (New York: Verizon, June 2014), 41, [http://www.verizonenterprise.com/DBIR/2014/reports/rp\\_Verizon-DBIR-2014\\_en\\_xg.pdf](http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf).

63. Martin C. Libicki, “Why Cyber War Will Not and Should Not Have Its Grand Strategist,” *Strategic Studies Quarterly* 8, no. 1 (Spring 2014): 23–39, [http://www.au.af.mil/au/ssq/digital/pdf/spring\\_2014/Libicki.pdf](http://www.au.af.mil/au/ssq/digital/pdf/spring_2014/Libicki.pdf).

64. UN General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (New York: UN, 24 June 2013), 4, [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/68/98](http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98).

65. *Ibid.*, 6–8.

66. Louise Arimatsu, “A Treaty for Governing Cyber-Weapons,” in *4th International Conference on Cyber Conflict*, ed. C. Czosseck, R. Ottis, and K. Ziolkowski (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2012), 91–109, [http://www.ccdcoe.org/publications/2012proceedings/2\\_3\\_Arimatsu\\_ATreatyForGoverningCyber-Weapons.pdf](http://www.ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyber-Weapons.pdf).

67. DOD, *Department of Defense Cyberspace Policy Report*, 8.



68. Kevin G. Coleman, "Aggression in Cyberspace," in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, ed. Scott Jasper (Washington, DC: Georgetown University Press, 2012), 109–16.

69. Aditya Balapure, "Cyber Weapon of Mass Destruction—The Blackhole Exploit Kit," *INFOSEC Institute*, 2 May 2013, <http://resources.infosecinstitute.com/cyber-weapon-of-mass-destruction-the-blackhole-exploit-kit/>.

70. H. E. Yun Byung-se, Minister of Foreign Affairs, "Statement by the Conference Chair" (Seoul Conference on Cyberspace, Seoul, South Korea, 17–18 October 2013), <http://www.mofat.go.kr/english/visa/images/res/StatementbytheConferenceChair.pdf>.

71. Executive Office of the President, "Fact Sheet: US–Russian Cooperation on Information and Communications Technology Security" (fact sheet, Washington, DC, 17 June 2013), <http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol>.

72. Ellen Nakashima, "Indictment of PLA Hackers Is Part of Broad U.S. Strategy to Curb Chinese Cyberspying," *Washington Post*, 22 May 2014, [http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9\\_story.html](http://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html).

73. Sui-Lee Wee, "In Cyber Spying Row, Chinese Media Call U.S. a 'Mincing Rascal,'" *Reuters*, 21 May 2014, <http://uk.reuters.com/article/2014/05/21/uk-cybercrime-usa-china-media-idUKKBN0E107K20140521>.

74. Robert S. Dewar, "The Triptych of Cyber Security: A Classification of Active Cyber Defense," in *Proceedings 6th International Conference on Cyber Conflict*, ed. P. Brangetto, M. Maybaum, and J. Stinissen (Tallinn, Estonia: CCD COE, June 2014), 7–21, [http://www.ccdcoe.org/cycon/2014/proceedings/d1r1s9\\_dewar.pdf](http://www.ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf).

75. Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Forces Quarterly* 73, no. 2 (2014), 12–19, [http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73\\_12-19\\_Williams.pdf](http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-73/jfq-73_12-19_Williams.pdf).

76. James P. Farwell and Rafal Rohozinski, "The New Reality of Cyber War," *Survival: Global Politics and Strategy* 54, no. 4 (August–September 2012), 110, <https://www.iiss.org/en/publications/survival/sections/2012-23ab/survival--global-politics-and-strategy-august--september-2012-f9ce/54-4-09-farwell-and-rohozinski-6b6d>.

77. Franklin D. Kramer and Melanie J. Teplinsky, "Cybersecurity and Tailored Deterrence" (issue brief, Atlantic Council, Washington, DC, December 2013), 6, [http://www.atlanticcouncil.org/images/publications/Cybersecurity\\_and\\_Tailored\\_Deterrence.pdf](http://www.atlanticcouncil.org/images/publications/Cybersecurity_and_Tailored_Deterrence.pdf).

78. Jeffery Carr, "Cyber Laws May Need Tweaking," *SC Magazine*, 3 December 2012, <http://www.scmagazine.com/cyber-laws-may-need-tweaking/article/268650/>.

79. Irving Lachow, "Active Cyber Defense: A Framework for Policy Makers" (policy brief, Center for a New American Security, Washington, DC, February 2013), 1–10, [http://www.cnas.org/files/documents/publications/CNAS\\_ActiveCyberDefense\\_Lachow\\_0.pdf](http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf).

80. 18 US Code § 1030—*Fraud and Related Activity in Connection with Computers*, <http://www.gpo.gov/fdsys/pkg/USCODE-2010-title18/pdf/USCODE-2010-title18-partI-chap47-sec1030.pdf>.

81. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2012), 204–05.

82. Hexis Cyber Solutions, "HawkEye G: The Active Defense Grid" (fact sheet, Hexis Cyber Solutions, Hanover, MD, 2013), <http://www.hexiscyber.com/products/hawkeye-g>.

83. US Joint Staff J-7, "Foreword," in *Unity of Effort Framework Solution Guide* (Suffolk, VA: DOD, 31 August 2014), [http://www.dtic.mil/doctrine/doctrine/jwfc/uef\\_solution\\_guide.pdf](http://www.dtic.mil/doctrine/doctrine/jwfc/uef_solution_guide.pdf).

84. Executive Office of the President, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communication Infrastructure* (Washington, DC: White House, May 2009), i.

85. Ministry of Defence, United Kingdom, "The Comprehensive Approach," Joint Discussion Note 4/05 (Shrivenham, UK: Joint Doctrine and Concepts Centre, 2006), 1-4-1-5, [http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.arcc.nato.int%2Fsystems%2Ffile\\_download.ashx%3Fpg%3D3313%26ver%3D1&ei=fYqtVL-IMYiyggTulYPoAw&usg=AFQjCNEF5Hllu9tO\\_UUFuwzRhg7aludNtg&sig2=wAbfdmhadcjpikYwAlz9fg&bvm=bv.83134100,d.eXY](http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.arcc.nato.int%2Fsystems%2Ffile_download.ashx%3Fpg%3D3313%26ver%3D1&ei=fYqtVL-IMYiyggTulYPoAw&usg=AFQjCNEF5Hllu9tO_UUFuwzRhg7aludNtg&sig2=wAbfdmhadcjpikYwAlz9fg&bvm=bv.83134100,d.eXY).

86. NATO, "A Comprehensive Approach," 27 October 2010, [http://www.nato.int/cps/en/SID-3F43C5C6-1F3BD449/natolive/topics\\_51633.htm?blnSublanguage=true&selectLocale=uk&submit=select](http://www.nato.int/cps/en/SID-3F43C5C6-1F3BD449/natolive/topics_51633.htm?blnSublanguage=true&selectLocale=uk&submit=select).

87. Executive Office of the President, *The Comprehensive National Cybersecurity Initiative* (Washington, DC: White House, 5 March 2010), 5, <http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf>.

88. Michael Hallet and Oke Thorngren, "Attempting a Comprehensive Approach Definition and Its Implications for Reconceptualizing Capability Development," in *Capability Development in Support of Comprehensive Approaches: Transforming International Civil-Military Interactions*, ed. Derrick J. Neal and Linton Wells II (Washington, DC: National Defense University, December 2011), 36, [http://mercury.ethz.ch/serviceengine/Files/ISN/142718/ipublicationdocument\\_singledocument/f6211158-d4b8-4e9b-ae68-c719f6e3a404/en/full+text.pdf](http://mercury.ethz.ch/serviceengine/Files/ISN/142718/ipublicationdocument_singledocument/f6211158-d4b8-4e9b-ae68-c719f6e3a404/en/full+text.pdf).

89. Larry Clinton, "Cyber Security Social Contract," in *Conflict and Cooperation in the Global Commons: A Comprehensive Approach for International Security*, ed. Scott Jasper (Washington, DC: Georgetown University Press, 2012), 185-98.

90. European Union, "International Code of Conduct for Outer Space Activities," version 16 September 2013, 1-12.

91. Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar," *Foreign Affairs*, 21 November 2012, <http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar>.

92. Jennifer O'Mahony, "Stuxnet Worm 'Increased' Iran's Nuclear Potential," *Telegraph* (UK), 15 May 2013, <http://www.telegraph.co.uk/technology/news/10058546/Stuxnet-worm-increased-Irans-nuclear-potential.html>.

93. Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling* (Carlisle, PA: Strategic Studies Institute, US Army War College Press, April 2013), 43-54, <http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf>.

94. Bob Gourley, "Reference to Cyber Security 'Wake-Up Calls,'" *CTOvision.com* (web site), 30 November 2013, <https://ctovision.com/2013/11/reference-cyber-security-wake-calls/>.

95. James R. Clapper, *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community; House Permanent Select Committee on Intelligence, US House of Representatives*, 113th Cong., 2nd sess., 4 February 2014, 1, <http://www.dni.gov/index.php/newsroom/testimonies/203-congressional-testimonies-2014/1011-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community-hpsci>.

96. Catherine Herridge, "NSA Director: China Can Damage US Power Grid," *FoxNews.com*, 20 November 2014, <http://www.foxnews.com/politics/2014/11/20/nsa-director-china-can-damage-us-power-grid/>.
97. James G. Stavridis, "The Comprehensive Approach in Afghanistan," *PRISM* 2 no. 2 (March 2011): 65–76, [http://cco.dodlive.mil/files/2014/02/Prism\\_65-76\\_Stavridis.pdf](http://cco.dodlive.mil/files/2014/02/Prism_65-76_Stavridis.pdf).
98. Martin E. Dempsey, "Defending the Nation at Network Speed."
99. DOD, *Quadrennial Defense Review 2014*, 15.
100. Alan Zibel, "Few Cautions on Financial Threat from Lone Hackers," *Washington Wire* (blog) on *Wall Street Journal* (web site), 5 October 2014, <http://blogs.wsj.com/washwire/2014/10/05/few-cautions-of-financial-threat-from-lone-hackers/>.
101. Hugh Son and Michael Riley, "JP Morgan Password Leads Hackers to 76 Million Households," *Bloomberg News*, 3 October 2014, <http://www.bloomberg.com/news/2014-10-03/jpmorgan-password-said-to-lead-hackers-to-76-million-households.html>.
102. Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth, "JPMorgan Chase Hack Affects 76 Million Households," *New York Times*, 2 October 2014, [http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?\\_r=0](http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_r=0).
103. James Andrew Lewis, "Cyber Threat and Response: Combating Advanced Attacks and Cyber Espionage" (white paper, Center for Strategic and International Studies, Washington, DC, March 2014), 1–8, [http://csis.org/files/publication/140313\\_FireEye\\_White\\_Paper\\_Final.pdf](http://csis.org/files/publication/140313_FireEye_White_Paper_Final.pdf). These tactics are seen in Dragonfly, an ongoing cyberespionage campaign targeting the energy sector that began with malware in phishing e-mails to executives, shifted to the compromise of energy-related web sites, and continued with infection of legitimate software packages available for download by equipment providers; and Keith B. Alexander, Emily Goldman, and Michael Warner, "Defending America in Cyberspace," *National Interest* (November/December 2013), 24. While it is uncertain how damaging coordinated cyber attacks could be if mounted on a national scale, the Dragonfly campaign achieved sabotage capabilities that could have caused disruption to energy supplies.
104. US Strategic Command, *Deterrence Operations Joint Operating Concept*, version 2.0 (Washington, DC: DOD, December 2006), 7–27, [http://www.dtic.mil/doctrine/concepts/joint\\_concepts/joc\\_deterrence.pdf](http://www.dtic.mil/doctrine/concepts/joint_concepts/joc_deterrence.pdf).

# Remediating Space Debris

## Legal and Technical Barriers

*Joshua Tallis*

### Abstract

As with many international crises, the solution to space debris is far more complicated than the circumstances that created it. A host of legal, political, and technical considerations persists in making space debris a topic of frustration. Preventing future debris has been a rallying point for a number of spacefaring nations, but it remains a growing problem that encourages greater utilization of technology and personal responsibility among agencies the world over. Still, as long as trash continues to clutter the skies, the risk to national security and economy will persist. Thus, while attempts at debris mitigation are critical to positively impacting long-term sources of debris, such limited attempts do not offer a solution to the wider problem. Something must be done. But what?

\* \* \* \* \*

*Space.* The word says it all: a pristine expanse with boundless potential and enough room for anything we could throw at it. However, words can be misleading. Outer space may be nearly boundless, but the neighborhood we populate is not. Currently there are over 500 operational satellites in low earth orbit (LEO); there are about 80 operational satellites in medium earth orbit (MEO); and there are around 400 operational satellites in geosynchronous orbit (GEO).<sup>1</sup> Accompanying those working instruments are 17,000 pieces of catalogued debris in LEO, 1,000 pieces in MEO, and 1,000 pieces in GEO.<sup>2</sup> Every single one of those measureable space objects is hurtling around the globe at an astonishing 7–12 kilometers per second, topping speeds on the imperial

---

Joshua Tallis is manager for research and analysis at Security Management International (SMI), an intelligence services provider in Washington, DC. He coauthored articles in the *Journal of Counterterrorism and Homeland Security International* with SMI associates and is a contributor to *SpaceflightInsider.com*, an aerospace news web site. Mr. Tallis is a PhD candidate at the University of St Andrews' Centre for the Study of Terrorism and Political Violence.

This article courtesy of *Air and Space Power Journal—Africa and Francophonie* 6, no. 1 (Spring 2014).



scale of 15,000 miles per hour.<sup>3</sup> One need only conduct a Google image search for “satellite” to see that space, at least the part of it that we have to contend with, is far from spacious. Moreover, the repercussions of a crowded earth orbit have significant national security implications through the threat of space debris.

Such debris is a hazard not only to life on the planet but, as a loaded minefield, can also precipitate a considerable loss of critical infrastructure. Yet, there remains little progress in the remediation of space debris. This article aims to highlight some of the significant legal and technological barriers to implementing space debris remediation, with political considerations intermixed in both, concluding that alleviating legal restrictions is the best avenue for encouraging any meaningful focus on this risk.

Trackable debris, or orbital debris, is used as a catchall term for any nonoperational piece of hardware in orbit. Particulates can range from a detached screw to an entire dislodged booster. The smaller (1–10 centimeters) remnants of disintegrated and exploded satellites number in the millions, and despite being the size of paint chips can easily kill an astronaut on a space walk or rip a hole through the International Space Station. In addition, while fewer in number, larger pieces of space junk—such as decommissioned satellites or abandoned segments of flight vehicles—pose a considerable risk across LEO and to the constellations of tightly orchestrated satellites in GEO. Larger debris presents a greater future risk of fragmentation, and thus, their removal has a disproportionate positive impact on orbital stability. Antisatellite (ASAT) missile tests (such as the Chinese Fengyun ASAT test), orbital collisions (such as the Cosmos-Iridium crash), and jettisoned capsules are among the largest sources of these materials. So why should the United States care?

First, reentering material threatens infrastructure and people, potentially leaving a wake of destruction on Earth’s surface that, while sounding like science fiction, occurs far more frequently than is commonly believed. For example, in 1978, a Russian spy satellite (Cosmos 954) failed to separate from its nuclear reactor before reentry. Consequently, the Canadian arctic was littered with radioactive debris from the satellite crash. In 1979, the American Skylab space station descended uncontrolled, striking parts of Western Australia. More recently, four solid rocket motors crash-landed in Uruguay, Saudi Arabia, Thailand, and Argentina since 2001.<sup>4</sup> Second, the International Space Station is also

frequently at risk of damage, placing in danger the lives of astronauts onboard and in transit. By some estimates, over the course of a typical mission, space shuttles faced the risk of a 1-in-250 chance of being catastrophically damaged by a high-velocity micrometeor or piece of debris.<sup>5</sup> In the course of 100 missions, that risk would reach a cumulative 33 percent—an admittedly dramatic but illustrative assessment.<sup>6</sup> Finally, space junk has the potential to disable a host of satellites critical to global commerce, national defense, international navigation, and agriculture.

So why not simply send up the space vacuums and clean up the mess we have made? As with many international crises, the solution to this issue is far more complicated than the circumstances that created it. A host of legal, political, and technical considerations persist in making space debris a topic of frustration. Everyone agrees something must be done; very few agree on just what exactly that something is. Preventing the creation of future debris has been a rallying point for a number of spacefaring nations. However, it is a Band-Aid fix to a still growing problem, albeit a fix that encourages greater utilization of technology and personal responsibility among agencies the world over. Still, as long as trash continues to clutter the skies, the risk to national security and economy will persist. Some observers, like National Aeronautics and Space Administration (NASA) physicist Donald Kessler, even suggest an instance of critical mass at which time the abundance of debris material in LEO could cascade into perpetual chain-reaction accidents. This phenomenon has been termed the Kessler syndrome.<sup>7</sup> Reports being circulated by NASA's Johnson Space Center support at least some aspect of Kessler's theory; even had all launches stopped in 2005, the preexisting cloud of orbital trash was, at the time, large enough to continue creating debris faster than atmospheric drag could remove it.<sup>8</sup> Thus, while attempts at debris mitigation are critical to positively impacting long-term sources of debris from ASAT explosions and ejected mission modules, such limited attempts do not offer a solution to the wider problem. The overall clutter of catalogued debris would likely continue to increase even if satellite launches stopped tomorrow; something must be done. But what?

## **Legal Barriers**

In popular perception, technology is seen as an exponentially expanding industry that, much like Moore's law, continuously pushes its own

boundaries. Such rapid growth is infrequently, if ever, matched by an equal evolution in the legal framework that governs it. Consequently, the controlling space law and treaties are, in many ways, hindrances to addressing contemporary problems because of their obtrusively outdated nature. In 1967, the United States signed the Outer Space Treaty (OST), broadly defining the most significant Cold War aims of what was then a bipolar celestial contest. In 1968, the United States and USSR included an Astronaut Rescue Treaty to this agreement and, in 1972, the Liability Convention was added as another addendum. In 1979, both the Registration Convention and the Moon Agreement were final caveats to this body of international law.<sup>9</sup> Since then, governments have necessarily oriented space law around this paradigm, and the result has not always been favorable to meeting mounting contemporary challenges.

First and most significantly, as of 2006, no international agreement or UN document uses or defines the term “space debris.”<sup>10</sup> It is impossible to address a problem that is neither identified nor institutionally acknowledged. Concededly, Article IX of the OST condemns the harmful contamination of space, though it does so in a rhetorical fashion and without mechanisms for enforcement or clear understanding of what contamination means.<sup>11</sup> Aiding in the reluctance of states to engage in a discussion on this topic is the inclusion of Articles VI and VII in the OST. Together, these sections form a broad conceptualization of liability in which a state is not only liable for the material it launches, but is also liable for any orbital devices launched by nongovernmental entities within that state’s domestic borders.<sup>12</sup> In 1967, when the United States and the Soviet Union were the only two nations with serious space capabilities and their respective governments provided the launch sites and overall vision for the space industry, that clause was a minor matter. Today, with space technology an ever-growing component of global commercial activities and with increased commercialization (and eventual privatization) of the space community, Articles VI and VII heap an overwhelming degree of liability on states, given the prevalence of corporations currently in the space business.

Ironically, the similarly outdated 1972 Liability Convention further complicated the question of fault. This convention was an attempt to define negligence in a manner to encourage the international community to behave responsibly in space. However, for such an agreement to have any considerable impact on debris remediation, its tenets must

be straightforward and enforceable. The convention produced neither. The first and most critical question to answer in exposing liability is the identification of what objects were involved in a given collision. In 1972, tracking equipment did not exist to make any meaningful technological impact on these talks. And while today US Strategic Command's (USSTRATCOM) Space Surveillance Network has a far greater capability to detect and monitor orbital debris, this ability is far from perfect and is not universally accessible. Yet even if a claimant could accurately identify who was involved in an orbital collision, the issue of negligence still has to be determined. Legally, the last affirmative action a state takes in launching a satellite (sans standard station-keeping maneuvers) is deciding its orbital parameters; merely launching a satellite does not constitute negligence.<sup>13</sup> Some believe that Inter-Agency Space Debris Coordination Committee guidelines, expanded International Telecommunication Union (ITU) registration, or the standard practice of boosting payloads to graveyard orbits offer avenues for assigning fault against those who do not comply with such norms in the future. But to date, no dominant rules-based order has reached global consensus.

Finally, the Liability Convention leaves us without a clear answer as to what constitutes causation. There are no rules of the road in space—no way of telling who was driving in the wrong lane or who blew a red light (only GEO slots even require registration with the ITU). Furthermore, functional satellites can often maneuver small distances. If a nonoperational piece of debris struck an operational satellite that did not jettison (move out of the way), is that contributory negligence? So far, there are no firm answers to questions like this, and consequently, catastrophic events such as Fengyun continue to pollute near earth orbits, while the international community feels no legal compulsion to act. In reality, the Liability Convention was not convened with the intention of protecting space; it was a political treaty meant to solidify key national interests in still poorly understood technical and judicial fields.<sup>14</sup> Still, without a compelling legal (and consequently economic) incentive to patrol space, the remediation of refuse will continue to be purely a matter of lip service for most states.

For argument's sake, let us assume states genuinely wanted to fix this problem and agreed to uniformly address every issue raised thus far. Only a handful of nations have the capability to actually remove debris from LEO, MEO, and GEO (mainly the United States and Russia). Imagine,



in a joint project, that these states develop a clever mechanism for the remediation of medium- to large-sized nonoperational orbital material. Despite these efforts, according to both the OST and the Registration Convention, there is no such thing as salvage rights in orbit. Anything put into space remains the property of the entity that launched it—even if that property explodes into 5,000 pieces. It is therefore illegal to move or remove any object in space that does not belong to the launching state or state of registry—at least to do so without permission.<sup>15</sup> Article VIII of the OST, which embodies this rule, may therefore bar Russian or US efforts to clean up debris in this scenario. This is, of course, assuming states can even identify who owns a certain piece of debris, which, as noted, is not a simple task. And lest we forget, what if in the effort to clean up debris, we create more? In that circumstance, we would find ourselves back at the circular discussion on liability.<sup>16</sup>

As we can see, remediation of space debris meets its first major obstacle in the perplexing legal regime that makes incentivizing through liability and ownership laws ambiguous and difficult to enforce. To be sure, there are solutions being considered as pressure mounts to solve this worrisome problem. Damage-compensation funds, apportioning damages based on market-share liability, and fault-based standards for damages have all been suggested.<sup>17</sup> While none has achieved a consensus, the mere fact that such matters are under discussion is a promising indication that the issue of space debris remediation is gaining ground. However, until liability, ownership, causation, rules of the road, and negligence are clarified and orbital debris is officially codified as a problem, motivation for greater action will continue to languish.

This reluctance among states to interact within a maladaptive legal system surrounding the space environment, while expressed in the lethargy of international action, also finds roots in domestic political and defense considerations. Any conversation on the legislative regime cannot be disentangled from the rationale driving state actors. For many nations, reluctance on this subject is driven largely by the defense apparatus. In the United States, NASA and the Department of Defense (DOD) have historically partnered on the topic of debris mitigation and adhere to strict guidelines in an effort to help reduce space debris.<sup>18</sup> Such efforts have likewise passed the United Nations General Assembly, for simple enough reasons: everyone can agree that creating even more space junk is a bad idea. In addition, while the 2010 US National Space

Policy instructed NASA and the military to pursue research and development on debris remediation, the policy lacked any timetable, rendering the instruction functionally useless.<sup>19</sup> Additionally, the government has yet to seriously task any agency with actually performing any debris removal, adding to the confusion in Washington.<sup>20</sup>

One reason for this disinterest in remediation is a result of the types of technology space cleanup would produce. Similar to concerns over satellite maintenance craft, the ability to dock and tamper with another satellite or fragment thereof leads inevitably to issues of dual use in space technology. Dual use is a reference to the civil and military applications of a related hardware. For example, a craft that could patrol and collect small debris could similarly be tasked to deorbit components of satellites belonging to another nation or competitive entity. The DOD and its counterparts in major spacefaring nations such as Russia and China have no interest in promoting the growth of such capabilities. This is not because these agents favor orbital clutter but because space debris is so far favorable to the investment in a civil technology that invariably carries with it national security ramifications. As space trash nears critical mass, such priorities may shift. Until that time, those in favor of investment in space debris technology and legislation will continue to meet strong opposition among governments.

## **Technical Barriers**

So, what can be done about existing debris? The answer, on the hardware side, is some method of active debris removal (ADR), which is an industry moniker for “something.” Recent events, such as the Chinese ASAT test in 2007 and the collision of Russian (Cosmos 2251) and American (Iridium 33) satellites in 2009, have brought increased attention (and refuse) to the topic of debris remediation.<sup>21</sup> One cannot overstate how critical an issue debris has become as a consequence of these two instances. Together, they have increased trackable material by nearly one-third. In response, the technical community has been tasked, despite the immense barriers noted in the previous section, with exploring some realistic and economical ADR systems for deployment within a reasonable though unspecified timeframe. However, something seemingly as simple as requesting designs for ADR concepts is inevitably tied up in myriad technical and political considerations. This section

outlines some of the obstacles to technological innovation in this field, with a heightened focus on the impact of policy choices on the developing technology.

Technical developments in fields that project little to no short- or medium-range economic advantages do not tend to garner private resources. Some believe government research grants should fill this gap. This belief implies that, for better or for worse, political considerations directly affect where technology in such industries migrates. The impacts of this correlation are obvious in highly politicized debates on climate change or stem cell research. Moreover, despite the lower profile, this relationship plays just as significant a role in ADR investment. Because defense concerns and legal uncertainties motivate governments to defend the status quo, no profound government push has driven technological developments. Furthermore, even should political motivations converge to produce a discernable mandate for ADR research, engineers will inevitably face constricting parameters from defense agencies concerned about dual-use applications. For example, a giant laser (an actual suggestion) designed to heat up one side of a piece of debris, causing it to collapse out of orbit, is essentially a giant ray gun. If it can deorbit a decommissioned satellite, it can just as easily disable an operational one. Furthermore, assuming the existence of positive responses from the defense community, a favorable legal climate, and supportive American political will, there remains a point of debate regarding exactly what type of ADR projects merit the limited resources made available to the Defense Advanced Research Projects Agency and NASA. Such determinations would require prioritizing either the removal of smaller debris, which aids in safeguarding existing operational satellites, or the remediation of larger debris, which contributes to the long-term stability of orbital systems.<sup>22</sup> Arguments for the former stress the use of tight resources in addressing immediate issues. Small debris is difficult to track, and the number of individual pieces extends into the millions. Difficulty cataloguing and monitoring so much debris means that things like paint chips and loose screws present the greatest short-term threat to operational satellites. Arguments for the latter stress the projections that removing even as few as five of the highest-risk large pieces of debris can considerably stabilize the orbital environment.<sup>23</sup> Because actors can easily catalogue large debris, such materials present a more limited immediate threat. However, as noted above, the fragmentation potential

of a large piece of orbiting junk presents an outsized, long-term risk. This risk will inevitably need to be addressed, though the necessarily myopic nature of politics (and the presence of more pressing considerations) makes the seemingly simple task of removing only a handful of pieces of debris difficult. Similarly, policymakers face a related choice between targeted and dragnet technologies, each posing their own benefits and issues as well.<sup>24</sup> Dragnets are particularly useful after a catastrophe, cleaning up clusters of debris before they spread by capturing a large amount of material similar to a trawler dredging the ocean floor. However, dragnets may be as undiscerning as a dredge as well—inexact in what they collect. Targeted techniques may be more equipped to mitigate the chances of specific collisions. So, assuming all of the political, legal, security, economic, and prioritization problems can be addressed, what technology is currently available for research investment?

The first step in answering that question involves enhancing situational awareness in space. To date, only USSTRATCOM monitors space debris in anything resembling a comprehensive fashion, opening a host of ethics questions on its own. For example, is the United States obligated to warn a foreign company or country of an impending collision? However, this single monitoring task relies on aging technology to track only tens of thousands of the millions of pieces of man-made junk in space. In 2013, the US government scrapped an S-band radar system known as Space Fence, due to sequester constraints. This system was an attempt to upgrade some of the infrastructure the joint force uses to track space debris. In June 2014, government revitalized the program, awarding Lockheed Martin a contract of nearly one billion dollars to resume work on the project. The legacy tracking system can track debris around the size of a basketball in LEO. The proposed Space Fence will be able to track debris down to the size of a baseball or smaller.<sup>25</sup> This increased ability could result in the amount of catalogued debris shifting from nearly 20,000 to closer to 200,000.<sup>26</sup> Yet, no matter whether Space Fence survives future cuts, any attempt at debris remediation will require that USSTRATCOM be afforded the resources to continue combing software-based predictive models enhanced by a growing ability to spot-check more debris. Such a capability is a prerequisite to any attempts at remediation, as we cannot remove what we cannot find. Likewise, enhanced situational awareness contributes to alleviating a number of the technical issues plaguing the debate on liability.



Yet, eventually, debris remediation will require the physical removal or deorbiting of space debris, and there is no shortage of proposals on how to accomplish this. One popular concept being circulated is the use of a tether, utilizing either electromagnetics or momentum exchange. Such devices usually focus on larger debris, causing such materials to drop out of LEO or flinging them into graveyard orbits above GEO—much in the way an object tied to a rope can be sent flying. The electrodynamic variant has gained prominence recently, with a \$1.9 million grant from NASA to Star Technology and Research making news in March 2012.<sup>27</sup> The advertised layout of their ElectroDynamic Debris Eliminator (EDDE) used a fleet of twelve crafts launched into LEO, working in unison to grab debris and drag it to short-lived orbits before cascading out of circulation. The company, which has received other government grants in the past, projected that a fleet of this size could conceivably remove all current LEO trash over two kilograms within seven years.<sup>28</sup> Consequently, while this is a targeted system carrying with it the benefits of accuracy and control, it is designed to choreograph in such a manner that it produces the long-term benefits of a dragnet approach as well. Whether it can truly keep up with the natural increase of debris, whether deorbited material runs the risk of reaching the surface, and whether such a large and mobile fleet further increases the chances of collisions are questions still needing to be answered, leaving this regiment one among a host of uncrowned contenders for the title of panacea. It joins the ranks of lasers and harpoons in the ever-growing club of designs vying for a slice of the inevitable windfall to be made from a likely crisis. While just one example, the EDDE demonstrates the complexities involved at every level of technical development and the associated costs for even nonoperational prototypes.

Space is an incredibly hostile environment. No atmosphere, high radiation levels, extreme temperatures, and the remote aspect of operations all make remediation a technical issue of the highest complexity. Additionally, with costs so high, outcomes so uncertain, priorities so ambiguous, and technologies still untested, active debris removal will continue to linger at the mercy of political whim. Only after such uncertainties are settled can the arduous process of technical trial and error begin. Space cleanup will not be a quick fix, and scientists concerned about the immediacy of the crisis will undoubtedly continue to see solutions

pushed to the horizon until those who control the flow of funding are persuaded to make the necessary political and economic investments.

Finally, any discussion of the role of commercial aerospace cannot ignore the reality that private industry is a growing segment of the launch and payload market. NASA increasingly relies on commercial partners (Orbital Sciences Corporation and Space Exploration Technologies Corporation [the latter more commonly referred to as SpaceX]) to meet its resupply obligations for the International Space Station. The Boeing Company, Sierra Nevada Corporation's Space Systems, and SpaceX are also in competition to provide commercial American access to LEO, a capability the United States has lacked since the termination of the shuttle program in 2011. SpaceX announced in August 2014 that it had selected Brownsville, Texas, as the site of a private commercial spaceport, where the company intends to conduct upwards of a dozen commercial launches annually. With these developments as a backdrop, it is obvious that private corporations cannot simply look at space remediation as an industry cash cow. Aerospace companies must be included in a regime that fairly distributes the responsibilities of debris prevention and remediation in a way that meets their role in the modern system. Updating the Liability Convention could provide one framework with which to help expand the international legal and financial responsibilities of commercial launch companies. International bodies such as the International Telecommunications Union (a United Nations affiliate) offer yet another avenue within which policy makers can discuss this decidedly multinational issue. However, no matter the method for addressing the rights and responsibilities of private companies, any broader discussion of the legal and technical barriers to space debris remediation must recognize this is no longer solely a governmental issue.

## **Conclusion**

Space debris is evidently a complicated and inherently international topic, with direct ramifications for national security. However, with material and responsibility spread among multiple nations and liability a major cause of concern for every participant, solutions can only originate in a global forum. Policy makers can address technical issues with funding; funding for such projects comes from the political establishment; and the political establishment listens to lawyers and generals. The best

way to appease that core constituency is to reach a multilateral consensus on an international set of standards and programs that eliminate uncertainty and the fear of legal reprisal against those who seek to fix the problem. This is the capstone of barriers to space debris remediation. If nations could concur on fundamental negligence principles and rules of liability in this context, while uniting technologically (as they have done with the International Space Station) to respond to the issue, the remaining conflicts do not disappear, but they do become far more manageable.

In a joint venture, the DOD could monitor openly the capabilities of participating agencies. Furthermore, it is inevitable that most military communities will eventually see debris as an unavoidable threat to national security. Thus, the status quo will not survive. With the defense community on board, political support for ADR becomes sustainable. This consequently opens funding in the budget process, which large companies and entrepreneurs alike can manipulate to the gain of ADR research grants. Additionally, with an agreement on enforceable liability and causation standards, investment will likewise follow in enhanced monitoring and situational awareness capabilities. By establishing a coherent set of incentivizing ground rules, we expose the tangles of space debris remediation to realistic solutions. If the international community can come together, the cleanup of space refuse becomes a far more promising venture. Until then, space junk will continue to fill our horizon and remain among the greatest potential threats to America's critical infrastructure. ■■■

## Notes

1. Secure World Foundation, *Space Sustainability: A Practical Guide* (Washington, DC: Secure World Foundation, 2013), 8, [http://swfound.org/media/121399/swf\\_space\\_sustainability-a\\_practical\\_guide\\_2014\\_\\_1\\_.pdf](http://swfound.org/media/121399/swf_space_sustainability-a_practical_guide_2014__1_.pdf).

2. Ibid.

3. Noncatalogued debris is projected to be in the millions. Catalogued debris is only the material current sensors can measure and spot check.

4. NASA, "Reentry of U.S. Rocket Stage Above South America," *Orbital Debris Quarterly News* 15, no. 3 (2011): 3. In none of these cases were lives lost, but they do represent the periodic (if infrequent) occurrence of dangerous reentries.

5. John Matson, "U.S. Taking Initial Steps to Grapple with Space Debris Problem," *Scientific American*, 31 August 2011, <http://www.scientificamerican.com/article.cfm?id=orbital-debris-space-fence>.

6. Ibid.

7. Kessler's calculations have been misapplied in pop culture, but the theory remains both viable and accepted as a theoretical scenario. In 2010, Kessler explained his updated position on the syndrome, and his general support for the model it produced, in the following paper: Donald Kessler, Nicholas Johnson, J. C. Liou, and Mark Matney, "The Kessler Syndrome: Implications to Future Space Operations" (paper, 33rd Annual American Astronomical Society Guidance and Control Conference, Breckenridge, CO, 6–10 February 2010), <http://webpages.charter.net/dkessler/files/Kessler%20Syndrome-AAS%20Paper.pdf>.

8. NASA Orbital Debris Program Office, "Orbital Debris Remediation," Johnson Space Center web site, 21 August 2009, <http://www.orbitaldebris.jsc.nasa.gov/remediation/remediation.html>. A study referenced by NASA concludes that the collision of satellites already in orbit by 2005 would eventually be enough to replace and exceed the amount of debris greater than 10-cm that would be lost to atmospheric drag. In other words, for every piece of debris that burned up in the Earth's atmosphere, new accidents would create at least one new piece of debris, even if we never launched another payload into space again.

9. Secure World Foundation, *Space Security Index, Space Security 2010: Executive Summary* (Washington, DC: Secure World Foundation), 12, <http://swfound.org/media/29036/ssi2010executivesummary.pdf>.

10. Michael W. Taylor, "Orbital Debris: Technical and Legal Issues and Solutions" (L.L.M. thesis, McGill University, 2006), 39–40.

11. *Ibid.*, 76.

12. *Ibid.*, 42.

13. *Ibid.*, 77.

14. The Convention on International Liability for Damage Caused by Space Objects (Liability Convention for short) entered into force in 1972—five years after the signing of the Outer Space Treaty. The convention's most fundamental provision is that all liability for a launch is held by the launching state. Consequently, only states can make claims against one another under the convention guidelines; corporations and individuals are precluded from doing so. In 1972, these were relatively uncontentious concepts, as only the super powers could even think of launching satellites into orbit. However, in an increasingly commercialized and vastly expanded industry, private companies play an undeniable role in the launching of payloads and the ownership and operation of satellites in orbit. As a consequence, a legal regime that holds states entirely financially responsible for the impact of actions of corporations or individuals launching from within their borders is one unlikely to be embraced by the international system. Equally, a regime that marginalizes an increasingly important community in the aerospace industry—commercial launch operators—is sure to be nonfunctional. In fact, despite 89 signatures, the convention has only ever been successfully used once, in the case of the Cosmos 954 crash mentioned earlier.

15. Taylor, "Orbital Debris," 80.

16. It is important to note that, no matter how significantly we address the inadequacies of the legal regime, collective action will always remain an obstacle to debris remediation. As with tackling climate change, cleaning space debris is an expensive project with little immediate prospects of financial gain for those actors who pay to address it. It is my position that an updated legal framework makes issues of collective action easier to discuss. Nevertheless, the fact remains that projects of collective origin and collective rectification are profoundly difficult political issues that, by definition, are not easily lent to simple solutions.

17. Taylor, "Orbital Debris," 85.



18. Dave Baiocchi and William Welser IV, *Confronting Space Debris: Strategies and Warnings from Comparable Examples Including Deepwater Horizon* (Santa Monica, CA: RAND Corporation, 2010), 83.

19. Matson, "U.S. Taking Initial Steps," <http://www.scientificamerican.com/article.cfm?id=orbital-debris-space-fence>.

20. NASA Orbital Debris Program Office, "Orbital Debris Remediation," <http://www.orbitaldebris.jsc.nasa.gov/remediation/remediation.html>.

21. Ibid.

22. Ibid.

23. Ibid.

24. Baiocchi and Welser, *Confronting Space Debris*, 46.

25. The new Space Fence will replace nine VHF-band radars with ground-based radar positioned on the Kwajalein Atoll in the Marshall Islands. The new detectors will use a compressed S-band to catalogue and spot check objects down to the size of a baseball in LEO.

26. Joshua Tallis, "Lockheed Wins Contract to Track Space Trash," *Spaceflight Insider*, 4 June 2014, <http://www.spaceflightinsider.com/space-flight-news/lockheed-wins-contract-track-space-trash/>.

27. Douglas Messier, "Company Gets \$1.9 Million from NASA to Develop Debris Removal Spacecraft," *Parabolic Arc* (blog), 12 March 2012, <http://www.parabolicarc.com/2012/03/12/company-gets-1-9-million-from-nasa-to-develop-debris-removal-spacecraft/>.

28. STAR, Inc., "ElectroDynamic Debris Eliminator (EDDE) Vehicle," n.d., <http://www.star-tech-inc.com/id121.html>.

# Power and Predation in Cyberspace

*Christopher Whyte*

## Abstract

This article offers an alternative framework for understanding the sources of national security and power online. Wide-scale deployment of cyberweaponry regularly occurs beyond the scope of direct attacks on the infrastructure of national security and has a real effect on the power potential of states in the international system. Though the threat of cyberattack is a potent one, the greater impact on state power stems from the long-term disruption and distortion of the national innovation economy. The integration of civil and industrial functions with network systems allows for unprecedented levels of access to those second-order processes that underwrite national innovative potential and, ultimately, national power. A disruption to this underlying national apparatus via persistent, intrusive computer network exploitations (CNE) could diminish the innovative growth potential of sovereign actors in international affairs along several lines and essentially produce a power potential deficit that would not otherwise have existed.



Can cyberweapons be used to alter the dynamics of global power? For many years, the answer to this question has been a resoundingly conditional one.<sup>1</sup> Certainly, the ubiquitous ability of state and nonstate actors alike to hack broadly with an ever-evolving set of digital tools offers support for the common notion that development of a significant and sophisticated digital establishment might benefit one or more global powers at the expense of others. The cyber domain—unlike the more traditional operating domains of sea, air, land, and space—offers actors the ability to affect and manipulate a man-made security environment defined wholly by the scope of those computer systems that are increas-

---

Christopher Whyte is a PhD candidate in the School of Policy, Government, and International Affairs at George Mason University. His research focuses on the intersection of technology, political behavior, and international security issues related to cybersecurity and the Asia-Pacific region. He is a WSD-Handa Fellow at Pacific Forum, Center for Strategic and International Studies, and has conducted research at several national security think tanks.

ingly at the heart of major socio-industrial processes. "Cyberweapons of mass destruction" that offer generic, far-reaching methods for shaping events in such environments could, in particular, supplement the abilities of geopolitical competitors as to affect a real change in the global balance of power.

However, the technical and organizational complexities involved in harnessing such processes on a large scale are significant. Although it seems fair to think broad-scoped digital weapons are likely to play an enabling role in any future conflict involving computer-assisted forces, the question of utility and lasting effect remains. If digital aggression is unable to cause lasting destruction or achieve permanent victories without a broader application of state capabilities, then could the capacity for launching massive cyberattacks really affect agent power in international affairs?<sup>2</sup>

Despite the emergence of a sizable body of analytic and technical work linking knowledge of network technologies to national security issues, attempts to explore this and related questions have been relatively unidimensional in considering the relationship between state power and cyberspace. Studies that focus on the nature of network-constituted capabilities as impactful in world affairs rarely stray from the idea of power diffusion. For instance, authors like Joseph Nye suggest that the unique meaning of network developments for power dynamics lies with the increased capacity of lesser actors.<sup>3</sup> Though useful for certain types of strategic analyses, this kind of assessment does little to speak to the broad-scoped nature of new technologies as increasingly synonymous with most mechanisms of social, commercial, and governmental capacity in the modern world. Cyberspace is not only an operational domain within which elements of the overt national security apparatus exist; it is also an avenue for access to national potential at a more fundamental level.

The purpose of this article is to develop a strategic understanding of the ways in which digital developments relate to creating and mobilizing power in both latent and societal terms. This is an alternative narrative of strategic power derived from network processes that rely on particular dynamics of interdependence and collective behavior at micro and macro levels. The central claim is that wide-scale deployment of cyberweaponry regularly occurs beyond the scope of direct attacks on the infrastructure of national security and has a real effect on the power potential of states in the international system. Though the threat of cyber-

attack is a potent one, the greater impact on state power stems from the long-term disruption and distortion of the national innovation economy.<sup>4</sup> Integrating civil and industrial functions with network systems allows unprecedented levels of access to those second-order processes that underwrite national innovative potential. Disrupting this underlying national apparatus via persistent, intrusive CNE, could diminish the innovative growth potential of sovereign actors in international affairs along several lines and essentially produce a power potential deficit that would not otherwise have existed.

The first consideration is the nature of cyberweaponry, noting the distinction between cyberweapons of mass destruction (CWMD) and mass effect (CWME). Next, the predator-prey model is used to describe the basic logic of interaction in international affairs and to explore the potential capacity-altering ability of CWME. Discussion centers on the implications of CWME deployment for state power, before looking at the incentives of involved agents. Another troubling reality—the inability to perfectly control such practices—is likely to interact with the incentives of different domestic actors to frustrate both governmental and intergovernmental efforts aimed at threat mitigation. This article concludes with a discussion of implications for governance and future research.

## **Cyberweaponry and Massive Effect**

Why are cyberweapons generally considered to have the potential for massive effect and, thus, the potential to directly influence power dynamics? It is certainly the case that digital instruments lack a singular function. Unlike nuclear weapons, where the potential for massive strategic impact stems very clearly from the destructive potential of the bomb itself, the shape of digital methods of incursion and destruction depend very acutely on the technical environment in which they are deployed. As such, the label of weapon of mass destruction might appear to be an inaccurate or, at the very least, an incomplete one. This is reflected in the policy making and operational environment in which the use of cyberweapons is made possible, with decision makers forced to consider the unique technical dynamics of a target environment in such a recurring fashion as to make the strategic value of a specific given digital tool inconsistent over time. Both evolutionary and revolutionary



systems development constantly alters the operational nature of the particular challenges facing analysts and officials, with the result that policy often accommodates situation-specific cyberweapon deployments rather than massive ones.

Nevertheless, cyberweapons and any digital instrument of manipulation have clear utility for massive effect deployments. One rationale is that cyberattacks, regardless of the technical shape or the manner of delivery of the payload, can and might be targeted at network processes that control, regulate, or coordinate the function of massive or massively dispersed systems. Today, concepts of digital arsenals most common to punditry and scholarship consider CWMD in much the same way we think of nuclear weapons—as instruments of destruction or incursion operationally defined by the scope of the desired outcome.<sup>5</sup> An example of such a WMD-style cyberattack would be the oft-cited threat of disruption to national power grids in which a vulnerability is exploited to shut down electrical networks across a nation.<sup>6</sup> Such an attack would lead to a widespread and far-reaching, disastrous outcome. Unsurprisingly, observers consider the types of payload needed to accomplish such an attack to be highly complex, technically sophisticated and deviously deployed at opportune times. One might say the same of nuclear or other WMD.

Another reason why we might consider cyberweapons to have massive effect potential has to do not with the scope of an intended outcome but rather with the scope of a given implemented incursion as one that is far-reaching.<sup>7</sup> Though an online arsenal that is deployed to achieve a massively destructive attack on, for example, an energy grid or nuclear facility is certainly of great concern, it is unquestionably the case that cyberweapons are increasingly deployed to undertake long-term, low-level sorties across a significant number of computer systems.<sup>8</sup> Generic code and design attributes, much like those found during analysis of the Stuxnet program, lend themselves to adaptive programs that are able to accomplish numerous incursive tasks, while simultaneously avoiding detection and spreading smartly. Though the particular nature of deployment was likely a response to the specific defenses in place in Iran's nuclear complex, Stuxnet stands as a good example of this type of assault, in which broadly-defined behavioral parameters guided remote action across a wide range of digital environments.<sup>9</sup> Beyond the physical sabotage of industrial facilities like Natanz, such generically coded,

adaptable programs are also—and perhaps most often—found as spying assets or attempts to steal or corrupt valuable data.<sup>10</sup> Indeed, though CWME deployments are far less-closely linked to those major digital attacks that aim to overwhelm host systems, they are thought to constitute the bulk of aggressive cyber activities between countries around the world. Compared with the relatively small number of publicly reported, high-value attacks reported to have taken place against US entities in recent years, intellectual losses of more than \$338 billion per year have been accrued from cyber incursions. This suggests that theft and distortion of information in its various forms are massively worthwhile pursuits.<sup>11</sup>

In sum, the extant literature on cyberspace and national security places a significant focus on the potential for massive digital attack on highly specific systems. In cybersecurity terms, “mass destruction” refers to the targeting of particular critical systems with sophisticated payloads at opportune moments. This is the main typology of behavior undertaken by opponents in cyberspace most closely tied by analytic and scholarly work to power political outcomes, perhaps because cyberweapons are thought of as enablers for broader geopolitical actions—like Russian operations in Georgia and Ukraine. In contrast, outside of confined circles, policy makers have broadly overlooked weapons of mass effect (WME) as having the potential for significant effects on power dynamics in international affairs, despite the relatively more common employment of such weapons. Of course, there is a difference between cyberattack and cyberexploitation, but semantic differentiation is made at the functional rather than the strategic level of policy planning.

This analytic disregard is problematic. Scholars and policy makers require a fuller understanding of the effects of cyberweaponry on power politics in international affairs at the micro and macro levels, not least because professional study of such developments lends itself to a more discursive and, potentially, cooperative international arena. The distinction is an important one, because CWME more intimately reflects the massive scope of network integration in relation to state functionality at every level of national security. Using the predator-prey model offers a first step in understanding the effects of those low-level, wide-effect instruments of interaction that are less easily categorized as amenable to mass destruction.

## **Predators and Prey in Cyberspace**

How might observers best understand the affect, if any, of deployed CWME on power dynamics in international affairs? As previously noted, cyberspace remains remarkably unidimensional in the context of power in international systems. Nye and various others have regularly cited the greater relative abilities that digital capabilities award to relatively weaker, smaller actors in international affairs.<sup>12</sup> This idea of power diffusion simultaneously broadens and constrains the scope of debate on the subject of network technologies in saying that cyberspace is both a medium through which many actors can affect societal, economic, or security processes and an operating domain that has noteworthy limitations on possibilities for interaction and effect. It also inappropriately focuses debate concerning cyber capabilities on assessments of the character of governments, rather than on the strategic nature of the security environment. What do advancing network developments mean for different types of actors online? How might states adapt policies to deal with a proliferation of online threats from multiple vectors?

While, at the organizational level such questions are ultimately necessary, there is a need to revisit and consider questions of interaction in cyberspace if we are to construct an appropriate framework for fully understanding power dynamics and potentialities in the context of cyberweapons. Beyond one-time attacks on state infrastructure, broad-scoped network exploitations produce real long-term, value-added outcomes for aggressors online. This is particularly true when institutionally organized by an established authority. Theft of sensitive data endangers military preparedness and diminishes gaps between security competitors in political affairs. Moreover, theft of intellectual property and operational data on a massive scale curtails national potential as derived from a state's innovation infrastructure processes. In addition to the relatively intangible consequence of reduced soft power in the international system, theft reduces access to the various resources a country like the United States might call on as leverage to guarantee particular actions or more generally to underwrite credibility in political interactions. In short, the deployment of CWME portends considerable potential to reduce the power of vulnerable actors to extend power in a diplomatically coercive, institutional, and normative manner in the long term.

Commonly referenced in the natural sciences, the predator-prey model illustrates the potential effects of CWME on power dynamics in

the international system. Though a strict read of the model is not apt for broad analysis, it is useful as an example of the manner in which actors interact in a system where there exists a degree of dependence on performance and resources and where awareness occupies an important part of the calculus undertaken by decision makers. It is important to realize that the treatment of CWMEs on power dynamics is not an intrinsically pessimistic one, even though the prospect of long-term structural repositioning might suggest so. As with any assessable threat to national and international security dynamics, rational outcomes merely define the scope of possibility and allow actors to consider the operational environment with a degree of contextual comprehension.

### **Relativity and Process in International Affairs**

In world politics, actors at every level operate in a relative context. However, the metaphor is incomplete, as no actor can be assumed entirely predatory in nature nor can the complexities of the international system be described so simplistically. We might consider the lessons of the Lotka-Volterra model of interdependent predator and prey populations as exemplary of the relational nature of power.<sup>13</sup> When prospects are dependent upon the position of others, the ability to influence the strategic environment of a given system emerges from a combination of relative power differentials. If one considers the ever-increasing manner in which international political and security outcomes manifest as a function of various interdependent processes, there is little doubt the competitive behavior of one actor affects others to greater or lesser degrees. Indeed, this assumption is a staple of vast subfields of literature in political science and elsewhere.

As in the Lotka-Volterra model, interaction and abilities are functions of power as derived from second-order processes. Specific institutional power is the relative ability of an actor or population to survive and thrive. Rather than treat institutional power as the ability of some actors to defeat or significantly influence others through the extension of hard forces, such power is constrained in the long term via reference to the relative increase of each population. The birthrate of the predator group falls when there is overextension and a limited ability to survive off a reduced prey population. The birthrate of the prey group then rises again over time as predators experience slow population growth and lack the capacity to hunt effectively. Allowing for a certain broad degree



of balance in the population levels in a set system (i.e., not considering instances of mass importation of new actors, etc.), this leads to a cyclical rise and fall in the relative prospects of the two actors.

How does this relate to an understanding of international relations useful to our analysis of CWME? The “refresh rate” denoted by birth-rates in the Lotka-Volterra model reflects an assessment of relative strategic power and long-term power potential that is a common characteristic of policy practices in the history of realpolitik and major international conflict. In particular, the rise of Nazi Germany and the development of war plans in the 1930s are notable in that the role of latent power potential played an over-weighted role in influencing thinking on policy execution. The assessment of Adolf Hitler and much of the military leadership in Germany was that the Soviet Union (USSR), long considered to be the most immediate threat to German stability and prospects in a given conflict, would be increasingly difficult to combat.<sup>14</sup> Indeed, several historical studies have shown that Hitler believed the USSR—rapidly recovering from its civil wars and the horror of Joseph Stalin’s early reign—would have effectively improved its refresh rate of power production so as to be relatively unassailable by 1950.<sup>15</sup> This accelerated war-planning efforts and likely influenced the development of a France-first policy married with a showpiece nonaggression pact. At the same time, Hitler and other Nazi leaders rarely missed an opportunity to express their view that, though the USSR was a more immediate challenge, the long-term competition for global hegemony would be one against the United States—a nation whose massive latent industrial potential later prompted Winston Churchill to utter the words “so we have won after all,” upon hearing of the attack on Pearl Harbor.<sup>16</sup>

Thus, process-based, institutional power significantly underwrites the nature of systemic relationships and has historically had great influence on decision makers over time. Certainly, leaders and national security establishments necessarily premise many decisions on assessments of near-term threats to stability and prosperity. Moreover, incipient crises and the need to continually assess a changing operational environment—the latter a prominent characteristic of the diffuse, man-made cyber domain—incentivize the development of policies focused on a flexible ability to cope with emergent future challenges. But there is significant need to cast strategic operations in the context of the potential for changing dynamics. Long-term power differentials and potential

capabilities in the future depend very much on the present behavior of actors, with the result that present policies must reflect a commitment to strategic positioning beyond the scope of immediate concerns.

### **Building Blocks of Power and Cyberspace as a Strategic Concern**

Why consider the rise of CWME in the context of such institutional drivers of national power? In a nutshell, the notion of power as an institutional and developmental phenomenon is highly relevant to any discussion of cybersecurity and broader international security strategies in today's complex, globalized world because CWME are essentially designed as weapons of national sabotage. While the threat of deployed CWMD prompts consideration of various types of actions that must be undertaken to protect the integrity of national infrastructure and of military forces, CWME deployed on a large scale and able to flexibly utilize generically-designed digital tools have real value-diminishing effects on the power potential of different actors in the international system.

History bears out the fact that a state's geopolitical power and influence significantly comes from its ability to tailor economic processes toward national interests, and superior abilities to react and adapt in the international environment are largely derived from an ability to successfully cultivate an edge in innovative capabilities. In addition to common arguments that cite technological innovation as crucial in awarding certain states distinct hard-power advantages from revolutionary military capabilities, the postwar economics literature on national production and growth further pegs innovative capacity as a singularly important driver of market prosperity.<sup>17</sup> In more than just allowing for economic growth, a country's refresh rate determines the ability of a country to fuel future growth and maintain an innovative edge in global affairs. New intellectual property allows an increasingly unfettered ability to translate growth revenues into a more effective marketplace for the generation of robust intellectual, technological, and service-oriented products. Thus, in addition to an improved ability to produce powerful instruments of international operation, the better a nation is able to incentivize innovative growth, the better it is able to underwrite a future ability to offset static material outgrowths of foreign power. American hegemony in all things economic and security-related for the past seven decades is a reflection of this actualization of a structural ability to efficiently and

effectively leverage innovative potential to perpetuate an advantageous systemic position.

CWME that aim to steal or disrupt information, particularly intellectual property and operational specifics, dramatically offset the ability of a nation or bloc to leverage an innovative edge in international competitions. This is particularly the case if broad-scoped CWME are periodically deployed in incapacitation attacks to provide additional disruption to the regular processes of targeted institutions. Victim companies and other organizations are then forced to compete on a playing field increasingly chosen and manipulated by advantaged opponents, regardless of the original source of innovative potential. For victims, this portends a development spiral increasingly defined by potential and periodically actualized threats and a necessary counteroperation that itself distorts innovation potential. In some situations, as in the process of selling massive product lines or in maintaining technological advantages in particular exchanges, this has significant immediate value. Over time, this can produce industry- and market-wide ripple effects, as lost revenue fails to yield the returns needed for continued innovative development in the future.

Of course, in the broader context of prospects for success in international interactions, such value-diminishing actions undertaken on a wide scale curtail and constrain the ability of an actor to wield hard, economic, and soft power by reducing the assets available for the purpose of underwriting geopolitical gestures. Military development necessarily suffers from the reduced innovative potential of a struggling private sector and production efforts become less of a cutting edge approach as new projects reflect increasingly reactionary considerations. Additionally, the reduction of a competitive edge for national companies diminishes prospects in international business and shrinks the degree to which a state can access foreign markets and influence foreign actors. This, in particular, has the effect of lessening the ability of a country to underwrite promises made for either coercive or mediative purposes; threats and assurances essentially become less credible as the power potential of an actor to follow through falls away.

Moreover, beyond the cumulative effects of CWME for the domestic polity, the use of broad-scoped digital instruments of intrusion to steal and disrupt information and processes portends opportunity cost advantages for aggressors. After all, innovation and successful sectoral

operation are not without significant costs. Thus, stolen power potential from CWME deployment comes in the form of value-diminished investment for the victim nation/company and operational savings for an aggressor. Certainly, absorption and adaptation effectiveness diminish an aggressor's ability and benefit along these lines, but the potential is clear. Moreover, an aggressor might use the disruptive or information extraction capabilities provided by widely-deployed CWME to insulate itself from the significant uncertainties involved in investing to develop powerful national instruments for geopolitical influence. Avoiding the trial-and-error usually involved in the construction of both an effective national security apparatus and a strong private marketplace allows for programs that build on the earned successes of foreign actors and frees up funding for other national concerns, like social spending, military growth, or support for national economic development. Indeed, recent reports on the economic costs of cybercrime and espionage point to this fact—in essence a value-multiplier effect—as evidence of the gravity of major industry losses from digital attacks that otherwise might be pegged at no more than 2 percent of national income.<sup>18</sup> The benefits of a dollar stolen are thought to outweigh the gains of a dollar invested in research by as much as a factor of two.<sup>19</sup> And this multiplier effect has only been quantifiably considered in the aggregate; the explicit targeting of pivotal nuggets of intellectual capital might produce even greater advantages for aggressors.<sup>20</sup>

In sum, the spoils of nondestructive hacking could disproportionately sustain the ability of states, including potentially revisionist ones, to devote significant resources to areas of national interest. Though cyberspace is often considered to be its own operational domain, the fact of the matter is that networks intersect with societal processes at every level. Thus, beyond the use of digital pathways to mount destructive campaigns against actors in international affairs, broad-scoped instruments of intrusion and low-level systems assault are likely to have a real and measurable effect on the latent and institutional power available to states out into the future. Though power potential might appear as a diffuse variable relative to the immediate capabilities-based concerns most commonly considered by policy makers, cyberweapons present a strategic concern that is difficult to decouple from broader considerations of power and competition in international affairs. This is unavoidably so,



because the integration of network technologies with core and peripheral socioeconomic functions continues.

### **Governance and the Payoffs of CWME Deployment**

Since cyberweapons are developed and deployed diffusely in international society (i.e., not exclusively by states), it becomes important to ask if an appropriately concentrated effort to undermine foreign actors is a plausible strategic concern to be considered by policy makers. Answering this question requires a closer exploration of the incentives involved in developing and maintaining CWME arsenals and consideration of the positions of those agents—namely parochial organizations and government entities—whose actions might cumulatively constitute a regime.

An appropriate starting point for such an effort is also an odd one: the idea that centralized state manufacture and maintenance of aggressive CWME deployments cannot be assumed. The reason for this is simple: many incursive or predatory cyber campaigns are undertaken by private organizational or individual actors acting to better narrow interests. In most cases, central governments have appeared to lack the capacity to organize private society along such lines. Though relative gains produced by such efforts may ultimately benefit national processes and undergird national prospects for greater influence in world affairs, it is shortsighted to think that such a subversive and broadly diffuse regime is synonymous with policy at the highest level of strategic planning and decision making. Even in cases where this seems to be the case, the complexities involved in integrating multifunctional digital technologies across societies and government establishments suggests that any assumption of universality or adherence to centralized approaches is limited.

Given this, from where might potential support for established use of CWME on a national scale come? Can we expect such processes to be governed at all? At the most basic level, of course, development and utilization of offensive low-level digital techniques might originate wholly within the realm of private civil and industrial society. The ability of relatively weak actors and individuals to hack effectively and with little chance of getting caught alters the payoff structure involved in producing outcomes via illicit, rather than legitimate, means. Moreover, direct outside intrusion into agent concerns or knowledge of the strong possibility thereof can further tip the balance in favor of preemptively producing a CWME capability, as can the probable difficulties involved

in seeking reparation for technically complex attacks through legitimate channels. In simple terms, potential gains and knowledge of possible hard-to-attribute competitor defection portends equilibrium where pre-emption is rational.

It is also plausible that governmental efforts might drive such a regime in two different ways. First, governments might recognize the potential for national gains and construct explicit, if well classified, regimes for directing such efforts. This may be significantly more likely for countries where government controls extend effectively into industry and civil society. Indeed, various reports attribute the high-level linkages involved in China's military, government, and bureaucratic establishments as beneficial for implementing high-level policy initiatives on cybersecurity on a broad scale.<sup>21</sup>

Second, it is possible that governance of this diffuse, massive process of widespread incentive to seek advantage online occurs itself in a diffuse and self-interested manner. Though governments tend to adopt broad positions of balanced regulation in line with strategic and national interests, it is commonly the case that sectoral operation is dictated by the relationship between governmental subentities and private/civil sector actors. Organizations, like the Department of Commerce, are significantly incentivized to support private sector operations within the context of enumerated policy interests defined much more broadly than a particular strategic stance on an issue might be. Likewise, particular subsections of the political elite are motivated to support local and regional economic interests, while national security bodies with narrow charters inevitably find direct and tacit support for private actor-instigated CWME deployments fall in line with operating imperatives not bounded by the presence of a high-level strategic directive on such operations. Governance, in short, can occur as a sequential result of a distributed series of compensatory payoff structures. This proposition is perhaps far more valuable by itself than the broader prospect of state-led CWME initiatives. The incentive-based emergence of such a regime merely requires some degree of diminished high-level control to play a role in motivating broad-scoped CWME intrusions.

### **Implications for Governance and Future Research**

The problem of CWME and the long-term potential for dynamic power shifts as a strategic concern suffers as much from distributed gov-

ernance issues as it does from the diffuse nature of the online environment. Affecting the regulatory control necessary for ensuring reductions in the development and deployment of CWME is likely to be as difficult as the challenging task of setting technical standards within which digital operators might simultaneously be protected and governed. Why? Quite simply, the incentive to hack is produced by the clear prospects for significant economic and circumstantial betterment that stem from CWME use. Moreover, motivation to hack is positively affected by the balance of attribution and other technological prospects that are likely to oscillate over time.

In the context of international cooperation and countermeasures that might be taken against the use of CWME, such difficulty in governing at home manifests in a significantly more foundational set of problems. Though greater cooperation for control of such regimes might be an obvious and desirable outcome, real progress is likely to face multitiered challenges on a recurring basis. First, as is often the case in international relations, verification of implementation of agreed frameworks and actions can be difficult when dealing with such a broad-scoped developmental issue. Governments are naturally secretive, and cyberspace is an area in which, due to the relatively ungoverned condition of public networks, programs and interests are closely guarded at the level of agencies. Second, in many cases, the gap between government policy making at the highest level and the instigation of new development or deployment of CWMEs at the level of substate actors can be immense. Trust in agreed frameworks or cooperative treaties would not only require credibility of process at the level of foreign government policy but also credibility of control over actors in those sectors of civil and industrial society that are, in addition to military or intelligence agencies, the real targets of any action. This may be problematic even in the case of government units, as national security outfits resist the constraints of narrow parameters for action and others argue for tight regulation to protect parochial interests. Finally, cooperation on this particular typology of cyberweapons—whether the particular circumstances describe cases of cyberespionage, cybercrime, or otherwise—is likely to require recurring review and an approach that emphasizes the need to alter framework procedures. After all, any success in regulating the deployment of such value-adding instruments will come into constant conflict with the inherent payoff motivations of continued development. The potential

payoffs of such low-end, high-gains cyber efforts represent a constant lure for government elements across a range of functions, again suggesting that broad-scoped cooperation is prone to defection.

So, how should policy makers approach the issue of CWME—as distinct from CWMD—and set about a diplomatic treatment of such a long-term challenge to national interests? Though further research may produce a more concise statement of policy recommendations moving forward, three clear angles of approach emerge. First, policy makers may find significantly more interest among foreign counterparts in cooperating on matters involving CWMEs that are generally considered to be unrelated to national power and process. These include incidents of cyber hacktivism by civil society groups distinct from oft-cited and accused examples of state incursion for political purpose, like North Korea's 2013 attack on South Korean television stations or Russian vandalism of Estonian political web sites in 2007. The hope for success here would be twofold. First, attempts to coordinate international anti-hacking efforts along narrowly-defined operational lines and boost multilateral observational capacities could constrain the relative ability of aggressive national agents to intrude without detection. Second, such an effort would aid in the development of international norms of behavior for low-level incursive activities in cyberspace, with the intended result of making coordinated condemnation of and action against broader CWMEs easier to achieve.

Second, policy makers and practitioners may find it easier to prosecute a campaign of counter-CWME development and deployment by focusing on those government and substate actors that have major reputational interests to consider. Multinational corporations, in particular, are likely prospects for any such regime, as the incentive to hack at any level contends with the need to maintain an ability to legitimately operate across multiple jurisdictions and within various markets.

Third, and perhaps most importantly, policy makers are likely to find progress more easily if broad cooperative efforts are underwritten and informed by an extensive and well-designed data collection and modeling program. Such a program could identify broader patterns in CWME activity (verified or suspected) and interact with data on national productive potential to produce quantifiable mechanisms for assessing CWME impacts, tipping points, and functionality. Such a program would be a first step in producing a national capability to effectively coordinate



on diffuse issues of cybersecurity and underwrite deterrent, compellent, and diplomatic efforts in interactions within and across borders.

It is not enough, of course, to simply prescribe an effective data regime to undergird national security policy-making efforts without recognizing the clear challenges involved. In particular, the cybersecurity field of analysts, scholars, and practitioners faces both parametric and motivational problems requiring broader research that interlinks existing bodies of knowledge in political science, military studies, and technical fields with the developmental realities of digital developments.

On the one hand, theory must catch up in such a way that policy makers might be afforded the ability to link complex ground truths with generalizable “systems of parts” that can provide insights appropriate for grand strategy planning. Then again, questions of incentives and data access must be broached in such a way as to effectively render information to which conceptual frames might be applied. Suggested voluntary data collection programs are a good start.<sup>22</sup> However, future efforts will need to contend with major issues. Notably, data fitted to theoretically derived models must match program requirements if robust results are to be had. This suggests that policy and rhetoric must work toward the goal of making data volunteering compatible with the self-interests of private actors—a task made particularly difficult by the need to match market and structural imperatives with strategic ones. It is critical that skewed availability of data should not, as it has in the past, act to distort strategic planning by emphasizing knowable incremental threats at the expense of relatively inaccessible ones.

In the end, it is perhaps most important to note that the various challenges presented by the existence of deployable CWME that could have a real impact on systemic power differentials are not intrinsically negative for states around the world. The dynamics described above do not, in themselves, portend an enduring arms race in the digital world in which actors at every level of society are unerringly motivated to participate. Certainly, developmental incentives and structural realities complicate the ability of policy makers and statesmen to coordinate and produce peaceable solutions to such national security woes. However, a legitimate cyber regime that “reduce[s] transaction costs and uncertainty” and acts to perpetuate appropriate norms of cooperation and mutual restraint would do much to counteract the negative effects of potential threats.<sup>23</sup> The task ahead for practitioners, as much as it is technical in

nature, is principally one of doing just that—transmuting the national benefits of such hacking and ensuring that cooperative certitude is a preferable option for self-interested actors in geopolitical affairs. For this to occur, fuller understanding of the parameters of cyber phenomena, the theoretical and technical, is needed.

## **Conclusion**

Though cyberespionage and broad-scope intrusion make their way onto the pages of most cybersecurity literature and punditry these days, it is vital that we develop a strategic understanding of the potential costs and ramifications of sectoral and parochial behaviors as they apply at the highest level of international political considerations. The ramifications of doing so are more than just greater understanding of the evolution of the cyber phenomenon; they are a chance for better-constructed policy and the evolution of a more discursive environment for producing meaningful solutions to our most foundational security challenges. Significant research and data explication are needed in the future if analysts and scholars are to effectively reconcile questions of CWME and strategic initiative within the cyber ecosystem of states. The complexities involved in understanding the shape of competing market and institutional formats for organizing incursive actions portend much needed developments along several lines and speak to the evolution of the cyber field in security and political studies as one of multifaceted focus.

The arguments and suggestions made here are a first step toward expanding professional and scholarly thought along these lines. Key among the takeaways is the fact that low-level intrusion is not only possible; it is the norm for incursive interactions in cyberspace. CWME pose a threat to global power dynamics so distinctly different from more commonly considered digital instruments of sabotage that they require both separate consideration as a strategic artifact and a unique approach to professional and diplomatic engagement on the subject. Moreover, and perhaps more so than with “traditional” online national security concerns, CWME can be creatures of socioeconomic construction as easily as they are of defense establishments. Where strategies of CWMD prevention or deployment might require a concentrated series of complex efforts, the shape of CWME counterproliferation is likely to be one of broad state and institutional enterprise. ■■■

Notes

1. For the most comprehensive survey of the development of a cybersecurity literature as a subfield of the international security field of study, see Robert Reardon and Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature" (paper, 2012 ISA Annual Convention, San Diego, CA, 1 April 2012), [http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri\\_ISA\\_2012.pdf](http://ecir.mit.edu/images/stories/Reardon%20and%20Choucri_ISA_2012.pdf).

2. For a full summary of these arguments, see Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38, no. 2 (Fall 2013): 41–73, [http://www.mitpressjournals.org/doi/pdfplus/10.1162/ISEC\\_a\\_00136](http://www.mitpressjournals.org/doi/pdfplus/10.1162/ISEC_a_00136); and Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 5–32, <http://www.tandfonline.com/doi/pdf/10.1080/01402390.2011.608939>.

3. Joseph S. Nye, "Cyber Power" (paper, Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010), <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf>.

4. Scholarship on cybersecurity and international security has yet to fully develop a narrative understanding of the interconnections between markets, institutions, and various national processes. However, recognition that the innovation economy—i.e., the dynamics of interaction between productivity, infrastructure, and knowledge inputs that drive economic outcomes and incentives—might be distorted by digital manipulations on a broad scale is not new. See James Lewis and Stewart Baker, *The Economic Impact of Cybercrime and Cyber Espionage* (Washington, DC: Center for Strategic and International Studies, 22 July 2013), [http://csis.org/files/publication/60396rpt\\_cybercrime-cost\\_0713\\_ph4\\_0.pdf](http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf). Nevertheless, linkages remain woefully understudied.

5. This assumption is drawn from a number of recent works, perhaps the most notable of which is Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (Fall 2013): 7–40, [http://belfercenter.ksg.harvard.edu/files/IS3802\\_pp007-040.pdf](http://belfercenter.ksg.harvard.edu/files/IS3802_pp007-040.pdf).

6. For example, see James Adams, "Virtual Defense," *Foreign Affairs* 80, no. 3 (May/June 2001): 98–112, <http://www.foreignaffairs.com/articles/57037/james-adams/virtual-defense>.

7. This distinction is a notable takeaway from Ralph Langner's cornerstone work on the development of Stuxnet and related uses of cyberweapons. For examples, see Ralph Langner, *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve* (Arlington, VA: Langner Group, November 2013), <http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf>.

8. *Ibid.*, 4.

9. *Ibid.*, 22. For a thorough account of the discovery and exploration of Stuxnet, see Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired: Threat Level Blog*, 11 July 2011, <http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet>; and Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies* 22, no. 3 (2013): 365–404, <http://www.tandfonline.com/doi/pdf/10.1080/09636412.2013.816122>.

10. For a good description of the use of such tools in offensive operations, see William A. Owens, Kenneth W. Dam, and Herbert S. Lin, ed., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009).

11. See Executive Office of the President, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: White House,

2009), [http://www.whitehouse.gov/assets/documents/Cyberspace\\_Policy\\_Review\\_final.pdf](http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf). A 2013 Center for Strategic and International Studies and McAfee report estimates that, at time of production in July, annual costs to US persons and companies from cybercrime and espionage had run between \$24 billion and \$120 billion. See Lewis and Baker, *Economic Impact of Cybercrime and Cyber Espionage*, 5.

12. Nye, "Cyber Power;" Rid, "Cyber War Will Not Take Place;" and Mary Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly* 54, no. 2 (June 2010): 381–401.

13. Reference to the predator-prey relationship is not uncommon in the natural sciences. Described by a series of equations developed by Alfred Lotka and Vito Volterra in the early twentieth century, the relationship outlines the parameters of interaction and competition between two agents in a given system (usually given as wolves/foxes and rabbits). The basic assumption made in the model is that one agent (the wolves/foxes) is dependent on the other (rabbits) as a food source. This ties the prospects of both agents together by means of defining an environment of constrained resources. See Alfred J. Lotka, *Elements of Physical Biology* (Baltimore, MD: Williams & Wilkins Company, 1925); and Vito Volterra, *Variazioni e fluttuazioni del numero d'individui in specie animali conviventi* (Rome, Italy: Memoria Accademia dei Lincei, 1926), <http://bpfe.eclap.eu/eclap/axmedis/b/bd0/00000-bd05ae74-d168-4c92-9a65-4f461377f7bd/2/~saved-on-db-bd05ae74-d168-4c92-9a65-4f461377f7bd.pdf>.

14. Antony Beevor, *The Second World War*, 1st ed., (New York: Little, Brown and Company, 2012).

15. *Ibid.*, 108.

16. *Ibid.*, 289.

17. See Moses Abramovitz, *Resource and Output Trends in the United States Since 1870* (Washington, DC: National Bureau of Economic Research, 1956), <http://www.nber.org/chapters/c5650.pdf>; and Robert M. Solow, "Technical Change and the Aggregate Production Function," *Review of Economics and Statistics* 39, no. 3 (August 1957): 312–20, <http://faculty.georgetown.edu/mh5/class/econ489/Solow-Growth-Accounting.pdf>.

18. See Lewis and Baker, *Economic Impact of Cybercrime and Cyber Espionage*, 15.

19. *Ibid.*, 16.

20. *Ibid.*, 17.

21. See U.S.-China Economic and Security Review Commission, *2012 Annual Report to Congress* (Washington, DC: US Government Printing Office, November 2012), 147–51; U.S.-China Economic and Security Review Commission, *2013 Annual Report to Congress* (Washington, DC: US Government Printing Office, November 2013), 243–65; Jon Lindsay, *China and Cybersecurity: Political, Economic, and Strategic Dimensions* (workshops, University of California, San Diego, April 2012); and Bryan A. Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Falls Church, VA: Northrop Grumman Corporation for the U.S.-China Economic and Security Review Commission, March 2012), [http://origin.www.uscc.gov/sites/default/files/Research/USCC\\_Report\\_Chinese\\_Capabilities\\_for\\_Computer\\_Network\\_Operations\\_and\\_Cyber\\_%20Espionage.pdf](http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf).

22. See Karl Frederick Rauscher and Erin Nealy Cox, *Measuring the Cybersecurity Problem* (New York: East West Institute, 21 October 2013), [http://issuu.com/ewipublications/docs/mcp\\_final\\_10\\_22\\_2013/4](http://issuu.com/ewipublications/docs/mcp_final_10_22_2013/4).

23. James Wood Forsyth Jr., "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace," *Strategic Studies Quarterly* 7, no. 1 (Spring 2013): 93–113, [http://www.au.af.mil/au/ssq/digital/pdf/spring\\_13/forsyth.pdf](http://www.au.af.mil/au/ssq/digital/pdf/spring_13/forsyth.pdf).



# Fear and Learning in Tehran

## What Recent Psychological Research Reveals about Nuclear Crises

*Michael D. Cohen*

### Abstract

Recent psychological research has shown that experiencing fear, if people believe they have *some* control over the source of the fear, reduces their tolerance for risk. Leaders who experience fear of imminent nuclear war thereafter tend to reject these risky policies. Indeed, experiencing the fear of imminent nuclear war will cause leaders to avoid calculated and uncalculated risks. While the United States should work toward a comprehensive solution with Iran, using force would be not only risky but also counterproductive. If Iran developed the bomb, the use of force would be much less likely to succeed than the simplest policy of all: allowing Iranian political leaders to stop this behavior on their own.



The Iranian nuclear challenge continues to command attention in the news and within the diplomatic community. Despite the continuing negotiations with the Iranian government at Geneva, fierce debate persists over how to respond to the threat posed by the country's nuclear activities. Most experts believe these activities aim to create either a nuclear weapon or the capability to produce one. Some have pushed for a military attack to damage or destroy Iran's nuclear program, worrying that any permanent settlement would allow Iran to develop a secret breakout nuclear capability and continue to advocate the use of force if Tehran falls short of its Geneva commitments.<sup>1</sup> Others have hoped sanctions and diplomacy alone will keep Tehran a great distance from the bomb and believe a final settlement can permanently prevent the regime from developing it.<sup>2</sup> However, both sides share the underlying assumption that if Iran develops nuclear weapons or perhaps even the capability to

---

Michael D. Cohen is an assistant professor of political science at the University of Southern Denmark and was a visiting scholar at the Arnold A. Saltzman Institute of War and Peace Studies at Columbia University for the fall 2014 semester. He has published in *International Security*, *International Relations of the Asia-Pacific*, and *The Non-Proliferation Review*. He is currently completing a book manuscript on the sources and effects of nuclear emboldenment.

produce them, the situation would wreak medium- to long-term havoc in the Persian Gulf and wider Middle East as Iran pursues its revisionist agenda behind the cloak of its nuclear deterrent.

However, there is another possibility. James Lindsay and Ray Takeyh recently argued that while a nuclear Iran would be most dangerous “at first, when it would likely be at its most reckless, like other nuclear aspirants before them, the guardians of the theocracy might discover that nuclear bombs are simply not good for diplomatic leverage or strategic aggrandizement.”<sup>3</sup> The waxing and waning of the Iranian nuclear crisis over recent decades suggests that the country’s supreme leader, Ali Hosseini Khamenei, and his associates are still learning about what nuclear weapons might offer Iran. Indeed, global trends in the conflict propensity of nuclear powers strongly suggest that if Iran developed nuclear weapons, such a learning process described by Lindsay and Takeyh is much more likely than long-term brazen regional behavior.<sup>4</sup> Tehran may try to brandish its newly found nuclear weight around the region, but Khamenei and his associates will quickly learn that nuclear threats do more harm than good. Despite regular warnings that an Iranian bomb would undermine an already fragile Middle East, the fact is since the 1950s, states that have harbored intentions to revise major parts of their status quo—a desire termed revisionist—and have developed secure second-strike nuclear forces have quickly learned that nuclear weapons are not useful for changing their environments. Such states have then accepted their regional order.

One can partly attribute this great nuclear-learning phenomenon to the number and strength of US alliances throughout the world and the presence of adversaries equipped with nuclear weapons. However, nuclear learning mostly results from fear of imminent nuclear war, when leaders of new nuclear weapons states attempt to transform their status quo and cause a nuclear crisis. Recent psychological research has shown that experiencing fear, if people believe they have *some* control over the source of the fear, reduces their tolerance for risk. Beliefs about *no* control or *total* control reduce the effect of fear on risk.<sup>5</sup> Because leaders are likely to believe they have *some* control over whether nuclear war occurs in the context of calculated (i.e., territorial grabs) and uncalculated risks (i.e., inadvertent escalation and/or deliberate nuclear attack), fear of imminent nuclear escalation will tend to make leaders minimize risk and use nuclear weapons for deterrence rather than dangerous coercive strat-

egies.<sup>6</sup> As leaders of new nuclear powers push to transform their status quo, they are more likely to approach the nuclear brink and experience fear of imminent nuclear war.<sup>7</sup> Attempting to transform the regional status quo after developing nuclear weapons involves accepting the risk of a nuclear crisis and nuclear escalation. Leaders who do this and experience fear of imminent nuclear war thereafter tend to reject these risky policies, because the brain subconsciously associates *any* risky policy to the initiator. Indeed, experiencing the fear of imminent nuclear war will cause leaders to avoid calculated and uncalculated risks: land grabs, other *faits accomplis*, ultimatums and other coercive demands, and limited uses of force. Therefore, while the United States should work toward a comprehensive solution with Iran, using force if the regime is not forthcoming would be not only risky but also counterproductive. It would encourage Khamenei to respond with force if he had a bomb and would further encourage him to build one if he did not. If Iran developed the bomb, the use of force would be much less likely to succeed than the simplest policy of all: allowing Iranian political leaders to stop this behavior on their own.

### **Nuclear Dogs That Have Not Barked**

Former Undersecretary of State for Arms Control and International Security Robert G. Joseph echoed a widely held belief, when he claimed that nuclear weapons would “embolden the leadership in Tehran to advance its aggressive ambitions in and outside of the region, both directly and through the terrorists it supports.”<sup>8</sup> In theory, the more nuclear weapons have spread throughout the world, the more the danger of regional instability should have increased.

However, over the past six decades, nuclear proliferation has caused short periods of instability and conflict that have been followed by longer periods of peace and tentative cooperation. Experience with nuclear weapons and the experience of fear in a nuclear crisis moderates the higher conflict propensity of new nuclear powers.<sup>9</sup> The four years that followed the Soviet Union’s development of the ability to target the United States with nuclear missiles in 1959 were the most dangerous of the Cold War.<sup>10</sup> Nevertheless, Soviet challenges to major US interests in Berlin and Cuba substantially declined by 1963. China killed several Soviet troops on the disputed Zhenbao Island on the Ussuri River

in 1969, five years after developing nuclear missiles in 1964. However, China did not challenge Soviet positions in the region again and indeed has not used force against the Soviet Union anywhere since then.<sup>11</sup> After Pakistan developed nuclear weapons around 1990, fatalities in the Kashmir conflict increased from 30 in 1988 to nearly 2,000 in 1992 and more than 4,500 by 2001. During this period, Pakistan fought the 1999 Kargil War with India and engaged in a 10-month mobilized crisis in 2001–02.<sup>12</sup> However, fatalities in Kashmir have steadily declined since then, and by 2012 were almost at pre-1990 levels.<sup>13</sup> Indo-Pakistani relations have slowly but steadily improved as Pakistani president Pervez Musharraf and Indian Prime Minister Manmohan Singh authorized secret back-channel diplomacy that may have come close to concluding a final Kashmir settlement.<sup>14</sup>

International security experts have been unable to convincingly explain this remarkable trend. The first and most credible conventional explanation is that changes in the local or international balance of military power prevented territorial revisionism that was earlier permissible. US, Soviet, and Indian defenses were certainly consolidated after Soviet, Chinese, and Pakistani challenges, which made subsequent attempts at revanchism more difficult. However, no defenses could have prevented further challenges. Pres. John F. Kennedy could not have stopped Soviet premier Nikita Khrushchev from attempting to reinstall Soviet missiles in Cuba or issuing further Berlin ultimatums. Soviet premier Leonid Brezhnev could not have prevented further Chinese attacks on Soviet positions on Zhenbao Island. In addition, no Indian defenses could have prevented further Pakistani challenges in the rugged, mountainous peaks of Kashmir. The international balance of nuclear and conventional power hardly changed when Soviet, Chinese, and Pakistani challenges ceased.<sup>15</sup> Increased defenses, useful as they are, cannot account for this phenomenon.

A second conventional explanation is that while changes in the balance of military power may not have been very effective, the simple presence of nuclear weapons has been. Nuclear weapons threaten to wreak total destruction out of even limited conflict; so, nuclear powers should behave with extreme caution.<sup>16</sup> While nuclear powers have hardly behaved with reckless abandon, this caution is not immediate and has to be learned.<sup>17</sup> Before Soviet, Chinese, and Pakistani leaders learned to behave with the caution appropriate for nuclear powers, they pursued



policies that carried a real risk of nuclear war. The simple presence of secure second-strike nuclear forces cannot explain this variation: a constant cannot explain variation.

A third conventional explanation is that the undesirability of nuclear war prevents leaders from forcefully responding to regional aggression by nuclear powers. Moreover, the tendency for military organizations to develop doctrines and policies that diverge from the preferences of civilian leaders carries a real risk of accidental or unintended nuclear escalation. New nuclear powers have indeed tended to be dangerous.<sup>18</sup> However, the same experienced nuclear powers have not. Instead, they have accepted major parts of their status quos that earlier were deemed intolerable. Military doctrines have not yet caused nuclear war and have been most dangerous when civilian leaders have practiced revisionism.

Finally, many have pointed toward elite competition within these regimes as a source of their undesirable behavior. However, Khrushchev and Mao Tse-tung were at the peak of their political power within the Soviet Union and China respectively when these states' foreign policies were so dangerous.<sup>19</sup> It is unlikely Musharraf authorized the Pakistani intrusion into Kargil in 1999 as part of a political power grab, and the general controlled Pakistani policy toward India throughout the 2001–02 crisis. Although the regime in Tehran may be highly fragmented, it is likely that if Iran develops nuclear weapons, Khamenei will have as much control over Iranian foreign policy as Khrushchev, Mao, and Musharraf did over theirs. There is an imperfect correlation between elite politics and foreign policies of these states: whereas the former hardly changed, the latter fundamentally transformed.

## **Fear and Loathing**

A more convincing explanation for the moderating effect of experience with nuclear weapons begins with the familiar observation that nuclear weapons are poor instruments for coercive diplomacy.<sup>20</sup> However, the low coercive value of nuclear weapons says nothing about how leaders learn this. Leaders—especially those motivated to revise their regional order—are no more likely to immediately hit upon accurate answers here than they are to immediately learn about the coercive power of other military strategies or weapons. The historical record presented hereafter clearly shows leaders of revisionist states learn about

the coercive limits of nuclear weapons the way most people learn most things: personal experience.<sup>21</sup> It occurs in their own nuclear crisis rather than through a more systematic analysis of their adversary, region, or the historical record. Moreover, their initial belief that nuclear weapons might allow them to realize their otherwise elusive revisionist dreams causes their nuclear crisis. Fear is the relevant variable that causes these lessons about the limits of nuclear weapons over time. Nuclear crises cause enough fear to produce moderation of revisionist, new nuclear powers that no aggregation of military and economic power can realize. Thus, there is a systematic effect of experience with nuclear weapons on a state's conflict propensity.<sup>22</sup>

Numerous studies have found that the experience of fear causes people to reduce their acceptance of risk. Images that are known to cause fear under laboratory conditions, such as images of snakes or the September 11 attacks, routinely cause people to accept less risk in subsequent choices than those not shown the images. People's brains are hardwired to avoid future situations they perceive as similar to those that caused the initial fear experience. If leaders fear imminent nuclear war, they will avoid any policies they believe will likely bring them back to the brink. Leaders' successors will likely also have experienced fear and likely behave similarly. This effect of fear on risk is not generated by any amount of reading of history and is conditional on people believing they have some control over the source of their fear. Unsurprisingly, fear has little effect on risk when one believes they have little control over its source. Why run from the bear if you think you cannot escape it? When people experience fear and believe they have no control over its source, its effect on risk acceptance is slight. However, when people experience fear and believe they have *some* control over its source—as leaders in nuclear crises would—they become extremely unlikely to accept further risks. This risk aversion occurs in those areas that are perceived to cause similarly dangerous situations as those that originally caused the fear in other unrelated circumstances. While these insights come from the laboratory experiments cited above, it is also clear that the effects of fear are substantially greater when the subjects are world leaders rather than undergraduate students and when these leaders genuinely believe they have control over whether nuclear war erupts.

Although it is difficult to measure the experience of fear precisely, the historical record shows that when leaders develop nuclear weapons and

stumble into a nuclear crisis, the fear of imminent nuclear war is necessary for them to radically transform their foreign policies. If they attempt to transform their regional order through some combination of nuclear threats and salami tactics and do not experience fear of imminent nuclear war, they will likely continue with their aggression. A healthy respect for the danger associated with nuclear weapons is insufficient to cause them to reverse course. Knowledge about how nuclear powers might cause nuclear war will not suffice. Leaders must stare down the nuclear brink and expect imminent nuclear destruction within hours or days.

People take time to learn. It took Khrushchev almost four years from the development of nuclear missiles in 1959 to the Cuban missile crisis in 1962. Five years passed Mao's first 1964 nuclear test before the 1969 war scare. Pakistan developed nuclear weapons in 1990, and Musharraf did not experience fear of imminent nuclear war until May 2002. Of course, new nuclear powers are not all the same. The Soviet Union, China, and Pakistan differ in many obvious ways. Cold War Europe, East Asia in the 1960s, and South Asia in the 1990s exhibited important differences. Soviet, Chinese, and Pakistani leaders had different grievances and addressed them through different strategies. However, these differences conceal a striking similarity. Fear of imminent nuclear war had similar effects on Soviet, Chinese, and Pakistani aggression. Such fear made deterring revisionism by these powers much easier, because they were less inclined to accept the risk. While before experiencing fear they pursued dangerous policies that dragged them into nuclear crises, afterward they substantially moderated their aggression and largely resolved contested but otherwise unresolved issues. Despite stark differences in culture, ethnicity, history of previous conflict, and leadership personality, the experience of fear of imminent nuclear war was necessary to cause leaders to refrain from nuclear coercion.

### **Fight or Flight?**

The Soviet, Chinese, and Pakistani cases all involved leaders who believed they had some control over nuclear escalation when they experienced fear. It is clear Khrushchev, Mao, and Musharraf had supreme control over their respective countries and would have believed they had real leverage—but obviously not total control—over whether nuclear war occurred. The Soviet, Chinese, and Pakistani crisis years—in the

early 1960s, late 1960s, and early 2000s respectively—might seem to contradict the idea that fear causes revisionist states to back down. After all, these episodes constituted the most dangerous peak of crisis periods that almost plunged the world or specific regions into nuclear war. However, these cases are clear instances of fear of imminent nuclear war moderating reckless foreign policies. Indeed, it is likely that had these leaders not experienced fear of imminent nuclear war they would have continued in their revisionist ways.

Although the Soviet Union first tested a nuclear bomb in 1949, Khrushchev did not obtain the capability to reliably target the United States with nuclear missiles until a decade later.<sup>23</sup> One-way Soviet bombing runs were too vulnerable to North Atlantic Treaty Organization (NATO) air defenses, and Khrushchev's 1956 Suez crisis threat was all bluff.<sup>24</sup> Nevertheless, the Soviet leader believed nuclear threats would enable him to get his way in the Middle East, West Berlin, Cuba, and elsewhere. According to Khrushchev's son, Sergei, the Soviet leader learned that "the mere mention of nuclear-armed missiles had a powerful effect."<sup>25</sup> Indeed, these years were the most dangerous of the Cold War. In addition, throughout the two Berlin crises, Khrushchev did not experience fear of imminent nuclear war.<sup>26</sup> However, after President Kennedy announced the quarantine of Cuba on 22 October 1962, Khrushchev began to experience fear of imminent nuclear war. He claimed to his presidium colleagues, "We started out and then got afraid. . . . [Moreover,] the tragic aspect is that they might attack and we will repulse it. It might turn into a big war."<sup>27</sup> He likely worried that US forces would prevent the remaining Soviet ships and submarines that advanced toward Havana from proceeding and that Soviet retaliation would quickly escalate to nuclear war.<sup>28</sup> Khrushchev stated to the president of Czechoslovakia on 30 October 1962, "We were truly on the verge of war."<sup>29</sup> He proclaimed in early December 1962, "Of course I was scared. It would have been insane not to have been scared. I was frightened about what could happen to my country—or your country or all the other countries that would be devastated by a nuclear war. If being frightened meant that I helped avert such insanity then I'm glad I was frightened."<sup>30</sup>

Khrushchev learned of the danger of nuclear coercion not from history or abstract theory but from his own personal experience at the nuclear brink. After this experience, he not only refrained from attempting



to reinstall Soviet nuclear missiles in Cuba but also accepted the intolerable situation in West Berlin, offered concessions in stalled nuclear test ban negotiations, and accepted milder communist revolutions in Iraq and Laos. Where earlier he lashed out, after experiencing fear, he more passively accepted intolerable changes. Tacit cooperation and confidence building measures replaced coercive demands.

By February 1969, Soviet forward patrolling of the disputed Zhenbao Island had become more aggressive, and fighting had seriously wounded several Chinese troops.<sup>31</sup> After a Chinese retaliatory ambush in March caused 200 Soviet fatalities, Chairman Mao began to worry about a retaliatory Soviet nuclear strike and experienced fear of imminent nuclear war.<sup>32</sup> Extensive underground tunnels were built throughout the country, Chinese leaders were evacuated from Beijing, and military units were placed on high alert. Mao confided to his personal nurse that "China and the Soviet Union are now at war."<sup>33</sup> It is possible that Andrei Grechko, the Soviet defense minister who planned the 1968 invasion of Czechoslovakia under the pretext of Warsaw Pact training exercises, had threatened to punish China with a nuclear assault.<sup>34</sup> Mao's doctor recalled the August 1969 relocation of millions from the city to the country: "Remaining city residents were mobilized to 'dig tunnels deep' in preparation for aerial, possibly nuclear, attack."<sup>35</sup> That month, Mao concluded that "it is not good for all central officials to assemble in Beijing . . . [because] even one atomic bomb will kill many of us."<sup>36</sup> The evacuation of China's top leaders from the capital shortly followed. He worried the incoming flight carrying Soviet premier Alexei Kosygin, arriving ostensibly to restart negotiations, might turn out to be an ambush and placed specially trained battalions throughout the airport. On 18 October, when the Kosygin flight was expected to arrive, Chinese strategic missile forces were placed on their highest alert for immediate launch. People's Liberation Army units were ordered to a state of total readiness. At a meeting of generals from all regional commands and service arms to address readiness, the term most often heard in the meeting hall was "the coming Soviet surprise attack."<sup>37</sup> On 19 October, Mao's deputy, Lin Biao, remained fixated on the Soviet aircraft that was carrying the Soviet delegation to Beijing, demanding intelligence updates every few minutes and delaying his usual afternoon nap until the Soviet delegates had departed Beijing.<sup>38</sup> After the Kosygin talks safely concluded, Chinese forces were kept at full alert for another six months.

Moscow and Beijing subsequently agreed to conflict prevention and escalation reducing measures, and China has not used force against Soviet or Russian positions on Zhenbao or elsewhere since 1969.<sup>39</sup> Mao seems to have learned of the dangers of nuclear weapons not from history but from his own nuclear crisis with the Soviet Union.

After developing nuclear weapons in 1990, Pakistan had not fought a war with India for almost two decades. However, Islamabad substantially increased sponsorship of the Kashmir insurgency throughout the 1990s, started the Kargil War in 1999, and engaged in a ten-month mobilized crisis with India between 2001 and 2002. After Pakistani-supported insurgents killed 30 civilians at a military camp in Jammu in late May 2002, Indian prime minister Atal Vajpayee threatened Pakistan with an invasion to dismantle terrorist infrastructure. Pakistani president Musharraf responded in late May with three missile tests and threats of nuclear attack against an Indian invasion.<sup>40</sup> By the end of the month, Musharraf “hardly slept . . . [and] feared imminent nuclear war.”<sup>41</sup> During his 27 May presidential address to his nation, Musharraf claimed, “Pakistan is currently passing through a critical juncture. We are faced with a grave situation and we are standing at the cross road of history. Today’s decision will have serious internal and external effects on our future. . . . Tension is at its height.”<sup>42</sup>

On 1 June, in his first public speech after experiencing fear of imminent nuclear war, Musharraf proclaimed that leadership on both sides must realize the very dangerous nature of the situation and that there should be no miscalculation on either side.<sup>43</sup> He subsequently described the May crisis as “very close . . . [and] extremely tense because there were war clouds.”<sup>44</sup> In June 2003, he told the *Washington Post* that “two hundred percent, there won’t be war . . . [because of] the understanding of the leaders. We’ve fought three wars and we know the hazards of war.”<sup>45</sup> Musharraf made no such claims after the 1999 Kargil War and the December 2001 terrorist attacks on the Indian parliament. Indian and Pakistani English-language newspaper coverage of the South Asian crisis also suggests that Musharraf experienced fear of imminent nuclear war at the end of May 2002.<sup>46</sup> Pakistani newspaper coverage of the crisis during the last week of May was about eight-times greater than coverage in December 2001 when the Indian parliament was attacked. Coverage during the last week of May 2002 was between two-thirds and four-fifths of Pakistani coverage of the Kargil War between mid-June

and mid-July 1999, when the Indian army began to attack Pakistani positions, killed hundreds of Pakistani troops, and recaptured occupied territory.<sup>47</sup> That Pakistani coverage in May 2002 was almost as high as when hundreds of Pakistani troops were being killed in Kashmir at the height of the Kargil War suggests that the May crisis also captured much national attention. Musharraf learned of the dangers of nuclear coercion not from the Cold War or even the history of Indo-Pakistani relations but from his own experience at the nuclear brink.

While violence in the Kashmir insurgency after May 2002 did not disappear, it declined substantially.<sup>48</sup> However, 2012 was almost as dangerous as 1999. Many have argued that this Pakistani about-face was caused in fact by US pressure on Islamabad to rein in its support for Kashmiri insurgents in the aftermath of the September 11 attacks and the US war in Afghanistan.<sup>49</sup> US pressure on Musharraf indeed occurred during the same period he experienced fear, making it difficult to isolate the role each played in Musharraf's decision-making process. However, the problem with the US coercion argument is that Pakistan did not succumb to US pressure to rein in its support. After Pres. George W. Bush's heavy-handed threats, Musharraf paid lip service to appease Washington and Delhi but offered no meaningful concessions. Pakistani authorities handed no militants over to India, and many of the militants the Pakistanis did apprehend were later released. Moreover, the US coercion argument cannot explain why Pakistan pursued a policy of nuclear threats to realize its Kashmir goals before May 2002 but opted for secret diplomacy, confidence-building measures, and tacit cooperation thereafter. Pakistani policy in Kashmir during the decade since 2002 has simply been much more risk averse than in the decade before. Musharraf's experience of fear of imminent nuclear war in late May 2002 explains the dramatic turnaround.

### **Terrified in Tehran?**

One might argue these findings are not applicable to Iran, due to that country's unique culture and religion and its distinct geopolitical and economic motives to develop nuclear weapons. However, the fact is that almost all states that have developed nuclear weapons have stumbled into a crisis out of inexperience and then authorized more moderate nuclear strategies and foreign policies after a few years' experience. This

“experience effect” in the cases of the United States (in Korea), the Soviet Union (in Hungary), the United Kingdom (in Egypt) and France (in Algeria), cases in the late 1940s and early 1950s, are likely attributable to the early Cold War as well as nuclear weapons. It is not clear that fear played a role here, because the uncertainty associated with the early Cold War drove the conflict propensity of the new nuclear powers. However, all inexperienced nuclear powers since the late 1950s have found themselves in conflicts and wars either trying to revise a status quo (Soviet Union and Pakistan) or preventing and/or coercing a revisionist nuclear power from doing so (India). In China’s case, nuclear weapons seem to have emboldened the Chinese to respond more forcefully to aggressive Soviet patrolling of disputed territory. In some cases whether the new nuclear power is revising or defending the status quo is unclear, because many other factors are also changing in a particular region, for example Israel and South Africa. Nevertheless, the fact that countries as different as the Soviet Union in the early 1960s, China in the late 1960s, and Pakistan in the early 2000s exhibited strikingly similar variation in their fundamental choices of coercive or moderate nuclear strategies shows that the great nuclear learning phenomenon knows no cultural or geographic bounds even though these countries exhibit important differences. The effect of experience with nuclear weapons on the central elements of their nuclear strategies over time is striking.

We can predict the general contours of how an inexperienced nuclear Iran would behave based on a careful reading of similar trends in these earlier cases. Many have argued Iranian culture and religion suggest the regime would behave far more dangerously than earlier inexperienced nuclear powers. However, while most Iranians believe a uranium enrichment program is their natural right, public opinion regarding developing nuclear weapons is much more divided. Ayatollah Ruhollah Khomeini explicitly stated that Iran should not develop nuclear weapons. While some conservative leaders have spoken of the virtues of sacrifice for the nation, it is far from certain this would cause them to use nuclear weapons or authorize aggressive foreign policies that put the regime and country at risk. Iranian culture and religion are obviously different from those of other nuclear powers, but there are no reasons to expect the regime to be an exception to the historical rule. One might worry Iran would give nuclear weapons to terrorists, but it would have strong incentives not to forfeit control over such powerful weapons.<sup>50</sup>



Others might also argue that Iran's motivation for developing nuclear weapons differentiates it from other cases. Scholars have extensively debated the causes of nuclear weapons proliferation.<sup>51</sup> However, the fact remains, whether those states that have developed nuclear weapons did so because of defensive or offensive geopolitical ambitions, domestic politics, well-endowed science bureaucracies, global isolation, psychological biases, or nationalistic beliefs, leaders in all countries behaved in fundamentally similar ways over time when they were inexperienced with nuclear weapons. The relationship between a state's decision to develop nuclear weapons and what happens after development is tenuous. A partial exception to this rule is the extent to which Khamenei and his associates in the Revolutionary Guard are dissatisfied with the status quo in the Persian Gulf. They likely desire to end their state's regional and global economic and political isolation and to increase their influence over regional affairs and economic development.<sup>52</sup> They may wish to reduce US influence by increasing the cost of US presence in the region. The stronger these desires—either before or after developing nuclear weapons—the greater the likelihood of Iran harassing Persian Gulf tanker traffic, sponsoring Shiite groups around the region to undermine conservative Sunni states, and sponsoring attacks against US troops throughout the Persian Gulf. Iran might issue coercive threats to the United States or its regional allies. While the Iranian army is large, many of its forces are obsolete and are no match for Israeli or US forces in a conventional conflict. Nor would Iran be able to do much to threaten or destroy Saudi oil production.<sup>53</sup> However, if Iran develops nuclear weapons, fear of imminent nuclear war in a crisis is likely to cause Khamenei and his associates to rely on moderate nuclear strategies. Moreover, if an inexperienced nuclear Iran begins to demonstrate hubris in the region, a crisis, fear of imminent nuclear war, and more moderate nuclear strategies will follow irrespective of whether Iranian threats were directed at the United States or its regional allies. Direct threats against the US homeland may cause a crisis more quickly than threats against Israel, Saudi Arabia, or other US regional allies, but the likelihood of a nuclear crisis and the concomitant effects of fear of imminent nuclear war would be the same in both cases.

One can also argue that an Iranian bomb could unravel the nuclear nonproliferation regime. The causes of a Saudi or Turkish bomb and the impact of this on the nuclear nonproliferation regime are separate

questions that I cannot fully address here. However, the literature on the causes of nuclear proliferation suggests that whether an Iranian bomb would cause regional proliferation is far from clear. Policy makers have worried about this ever since Pres. Kennedy worried about 40 nuclear powers in the 1960s, but well into the twenty-first century, the number of nuclear powers remains below 10.<sup>54</sup> For example, while Saudi policy makers have often said they would develop nuclear weapons if Iran did so, much of this is designed to pressure the United States to prevent Iran from developing the bomb.<sup>55</sup> The United States has effectively used a combination of carrots and sticks to prevent many states from developing nuclear weapons, and it is not clear that an Iranian bomb would stop this trend.<sup>56</sup> Finally, one can argue that an Iranian bomb would undermine the global nuclear nonproliferation regime. Again, I cannot fully address that issue here, but the effect of the nuclear nonproliferation regime on states' decisions to develop nuclear weapons is contested.<sup>57</sup> Moreover, it is a stretch to assume that an Iranian bomb would have much effect on distant states' nuclear decisions. An Iranian bomb may well pose challenges to the global nuclear nonproliferation regime that are as similar and surmountable as those posed by the other nuclear powers.

In the long crisis over Iran's nuclear activity, the great nuclear learning phenomenon has all but gone unmentioned. The robust historical trend clearly indicates a need to guard against hasty conclusions that an Iranian bomb would wreak havoc throughout the Persian Gulf and Middle East. If Khamenei evades Israeli bombs and computer hackers, secretly develops nuclear weapons, and attempts to increase the cost of US influence in the region, there is little the United States and its allies could do to stop him short of military attack. Harassing Persian Gulf tanker traffic, undermining conservative Sunni regimes, and sponsoring attacks against US troops in Iraq and Afghanistan are not easily deterred. Thus, a growing number of policy makers and analysts have argued that military force should always be an option—one that may well be required if Iran developed nuclear weapons.<sup>58</sup> Nevertheless, an attack would likely cause Iran to double down on its nuclear program and may cause a regional war.

The custodians of any potential Iranian nuclear arsenal face a great obstacle to realizing their revisionist ambitions. Any attempts to reduce US influence in the region would likely cause US and/or Israeli reactions

that would eventually leave Khamenei and his associates fearing imminent nuclear war. Such fear caused Soviet, Chinese, and Pakistani leaders to cease their nuclear saber rattling, and it is unlikely Iranian leaders would react differently. If Iranian leaders believed a nuclear war was imminent, they would do whatever they could do ensure nuclear weapons would not be used. The historical record suggests that under these conditions Iranian foreign policy would come to resemble that of other experienced nuclear powers. It is also likely that Iranian foreign policy toward its other adversaries would show more signs of cooperation and confidence building and less signs of bluff and bluster. It is surely more difficult to establish whether Iranian leaders have experienced fear of imminent nuclear war than it is to count the number of challenges a nuclear Iran could pose to the United States and its partners. However, such an assessment is vital, because whether and how Khamenei and his associates experience fear of imminent nuclear war will determine if Iran throws its nuclear weight around the region and decide the manner in which the regime stops doing so. In the meantime, two broad lessons from the great nuclear learning phenomenon provide a more sober assessment of the situation.

If Tehran develops nuclear weapons, the first lesson is, the United States should not attack Iran. Imposing a nuclear crisis on new nuclear powers hoping to quickly cause the desired effects of fear through US threats or uses of force would be a dangerous mistake, because the desired effect of fear depends on beliefs about control. If Khamenei believes regime change is imminent, he will likely believe he has little control over nuclear escalation and the fate of his regime. He would be most likely to use nuclear weapons under these conditions. If Tehran developed nuclear weapons and attempted to revise the status quo through a combination of threats and smaller uses of force, the United States would not have to do much to cause Khamenei to learn of the limits of nuclear weapons to transform the Persian Gulf. Superior US military power can easily prevent Tehran from sustaining revisions to the status quo. Policy makers should reconsider any intelligence assessments that do not explicitly account for the impact of fear of imminent nuclear war on Tehran's behavior. Assessment after assessment has suggested that nuclear weapons would embolden Tehran to harass Persian Gulf tanker traffic, threaten or attack Saudi oil infrastructure, and increase sponsorship of attacks against US troops in Iraq and Afghanistan. Khamenei and his associates

may try to do this, but the historical record shows that the workings of the human mind will prevent them from getting very far.

The second lesson is that the United States should not threaten to attack Iran and would do well to announce it would only use force if Tehran first attacked US forces or perhaps those of key allies. US military power is so much greater than that of Iranian forces that if the US deployed forces in the region during a nuclear crisis, the mistrust and suspicion between Washington and Tehran may cause Khamenei to believe regime change was imminent. He would seriously consider using nuclear weapons under these conditions.

The best US deterrence policy would credibly commit to leave Tehran with some control over whether conventional or nuclear war erupts. US military assets deployed to the region should be much better at defending US and allied troops from Iranian challenges than invading and occupying Tehran. Khamenei would be much more likely to believe he had control over nuclear escalation and the fate of his regime during a nuclear crisis if he believed the United States would not attack unless deliberately provoked.

Traditionally, dealing with new nuclear powers has involved some combination of robust extended deterrence policies and threats to use force. However, revisionist new nuclear powers of the twenty-first century are likely to have very weak conventional military power. The dynamics of how people react to fear ensure that US threats to topple the regimes of these nuclear powers pose substantial dangers. The world is fortunate that leaders of new nuclear powers have been educated by fear and restrained their own revisionist ambitions. The United States and its allies must take care not to adopt policies thought to decrease the risk of nuclear war that actually make it more likely. If Iran develops the bomb, the best US approach would allow Iran to experience nuclear fear and learn to curtail their revisionist plans. ❧

## Notes

1. Matthew Kroenig, "Time to Attack Iran: Why a Strike is the Least Bad Option," *Foreign Affairs* 91, no. 1 (January/February 2012): 76–86, <http://www.foreignaffairs.com/articles/136917/matthew-kroenig/time-to-attack-iran>; and Matthew Kroenig, "Still Time to Attack Iran: The Illusion of a Comprehensive Nuclear Deal," *Foreign Affairs* (web site), 7 January 2014, <http://www.foreignaffairs.com/articles/140632/matthew-kroenig/still-time-to-attack-iran>.



2. Michael Jacobsen, "Sanctions against Iran: A Promising Struggle," *Washington Quarterly* 31, no. 3 (Summer 2008): 69–88, <http://www.washingtoninstitute.org/uploads/Documents/opeds/48441932e22c4.pdf>; Meghan L. O'Sullivan, "Iran and the Great Sanctions Debate," *Washington Quarterly* 33, no. 4 (October 2010): 7–21, <http://csis.org/files/publication/twq10octoberosullivan.pdf>; and Robert Jervis, "Getting to Yes with Iran: The Challenges of Coercive Diplomacy," *Foreign Affairs* 92, no. 1 (January/February 2013): 105–15, <http://www.foreignaffairs.com/articles/138481/robert-jervis/getting-to-yes-with-iran>.

3. James M. Lindsay and Ray Takeyh, "After Iran Gets the Bomb: Containment and Its Complications," *Foreign Affairs* 89, no. 2 (March/April 2010): 33–49, <http://www.foreignaffairs.com/articles/66032/james-m-lindsay-and-ray-takeyh/after-iran-gets-the-bomb>.

4. Michael Horowitz, "The Spread of Nuclear Weapons and International Conflict: Does Experience Matter?" *Journal of Conflict Resolution* 53, no. 2 (2009): 234–57.

5. The literature attesting to this effect is extensive. See Jennifer Lerner and Dacher Keltner, "Fear, Anger and Risk," *Journal of Personality and Social Psychology* 81, no. 1 (2001): 146–59, <http://socrates.berkeley.edu/~keltner/publications/lerner.fear.jpasp.2001.pdf>; Jennifer Lerner, Roxana M. Gonzalez, Deborah A. Small, and Baruch Fischhoff, "Effects of Fear and Anger on Perceived Risks of Terrorism: A National Field Experiment," *Psychological Science* 14, no. 2 (March 2003): 144–50; and Linda J. Skitka, Christopher W. Bauman, Nicholas P. Aramovich, and G. Scott Morgan, "Confrontational and Preventative Policy Responses to Terrorism: Anger Wants a Fight and Fear Wants 'Them' to Go Away," *Basic and Applied Social Psychology* 28, no. 4 (2006): 375–84.

6. One might argue that the dynamics of nuclear crises would lead leaders to believe that they have *no* control over whether nuclear war occurs. However, leaders are far more likely to believe that they have *some*—albeit not total—control. See Richard Ned Lebow, *Nuclear Crisis Management: A Dangerous Illusion* (Ithaca, NY: Cornell University Press, 1988) 97.

7. One might argue that we cannot know if leaders believed that they were at the nuclear brink. But if later scholars can identify the mobilizations and diplomacy that documented that nuclear war was imminent, leaders who authorized the mobilizations and diplomacy surely also believed that they were at or near the brink.

8. Robert G. Joseph, *Statement before the House International Relations Committee*, House of Representatives, 109th Cong., 2nd sess., 8 March 2006, <http://2001-2009.state.gov/t/us/rm/63121.htm>.

9. Horowitz, "Spread of Nuclear Weapons." 242–52.

10. For the argument that the Soviet Union developed nuclear missiles much later than usually assumed, see Matthias Uhl and Vladimir I. Ivkin, "'Operation Atom': The Soviet Union's Stationing of Nuclear Missiles in the German Democratic Republic, 1959," *Cold War International History Project Bulletin* 12/13 (Fall–Winter 2001): 299–307, [http://www.wilsoncenter.org/sites/default/files/CWIHP\\_Bulletin\\_12-13.pdf](http://www.wilsoncenter.org/sites/default/files/CWIHP_Bulletin_12-13.pdf).

11. M. Taylor Fravel, *Strong Borders, Secure Nation: Cooperation and Conflict in China's Territorial Disputes* (Princeton, NJ: Princeton University Press, 2008), 216. For evidence of Mao's 1969–1970 war scare, see John Wilson Lewis and Xue Litai, *Imagined Enemies: China Prepares for Uncertain War* (Stanford, CA: Stanford University Press, 2006), 48–72.

12. S. Paul Kapur, "Ten Years of Instability in Nuclear South Asia," *International Security* 33, no. 2 (Fall 2008): 71–94, <https://casi.sas.upenn.edu/sites/casi.sas.upenn.edu/files/iit/Ten%20Years%20-%202008.pdf>; and Michael D. Cohen, "How Nuclear South Asia Is Like Cold War Europe: The Stability-Instability Paradox Revisited," *Nonproliferation Review* 20, no. 3 (November 2013), 433–51.

13. Institute for Conflict Management, *South Asian Terrorism Portal* (web site), 30 November 2014, [http://www.satp.org/satporgt/p/countries/india/states/jandk/data\\_sheets/annual\\_casualties.htm](http://www.satp.org/satporgt/p/countries/india/states/jandk/data_sheets/annual_casualties.htm).
14. Steve Coll, "The Back Channel: India and Pakistan's secret Kashmir talks," *New Yorker*, 2 March 2009, <http://www.newyorker.com/magazine/2009/03/02/the-back-channel>.
15. Horowitz, "Spread of Nuclear Weapons," 242–52.
16. Kenneth N. Waltz, "More May Be Better," in *The Spread of Nuclear Weapons*, ed. Scott D. Sagan and Kenneth N. Waltz (New York: Norton, 2013), 3–40; John J. Mearsheimer, "The Case for a Ukrainian Nuclear Deterrent," *Foreign Affairs* 72, no. 3 (Summer 1993): 50–66, <http://johnmearsheimer.uchicago.edu/pdfs/A0020.pdf>; John Lewis Gaddis, "The Long Peace," *International Security* 10, no. 4 (Spring 1986): 99–142; Bruce Bueno de Mesquita and William. H. Riker, "An Assessment of the Merits of Selective Nuclear Proliferation," *Journal of Conflict Resolution* 26, no. 2 (June 1982): 283–306; David J. Karl, "Proliferation Pessimism and Emerging Nuclear Powers," *International Security* 21, no. 3 (Winter 1996–1997): 87–119; Jordan Seng, "Less is More: Command and Control Advantages of Minor Nuclear States," *Security Studies* 6, no. 4 (Summer 1997): 50–92; and Devin T. Hagerty, *The Consequences of Nuclear Proliferation: Lessons from South Asia* (Cambridge, MA: The MIT Press, 1998).
17. One might argue that those who believe in limited nuclear exchanges would be unlikely to experience fear of imminent nuclear war. However, limited nuclear war has never occurred, and leaders who experience limited nuclear war would likely experience fear of inadvertent escalation.
18. Scott D. Sagan, "More Will Be Worse," in *The Spread of Nuclear Weapons*, ed. Scott D. Sagan and Kenneth N. Waltz (New York: Norton, 2013), 41–81; Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton, NJ: Princeton University Press, 1993); Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington, DC: Brookings University Press, 1993); Bruce G. Blair, "Nuclear Inadvertence: Theory and Evidence," *Security Studies* 3, no. 3 (Spring 1994): 494–500; Peter D. Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States* (Ithaca, NY: Cornell University Press, 1993); Peter D. Feaver, "The Politics of Inadvertence," *Security Studies* 3, no. 3 (Spring 1994): 501–08; Steven E. Miller, "The Case against a Ukrainian Nuclear Deterrent," *Foreign Affairs* 73, no. 3 (Summer 1993): 67–80, <http://www.foreignaffairs.com/articles/48956/steven-e-miller/the-case-against-a-ukrainian-nuclear-deterrent>; Peter R. Lavoy, "The Strategic Consequences of Nuclear Proliferation," *Security Studies* 4, no. 4 (Summer 1995): 695–753; and Peter D. Feaver, "Neooptimists and the Enduring Problem of Nuclear Proliferation," *Security Studies* 6, no. 4 (Summer 1997): 126–36.
19. Aleksandr Fursenko and Timothy Naftali, *Khrushchev's Cold War* (New York: Norton, 2007); Roderick MacFarquhar and Michael Schoenhals, *Mao's Last Revolution* (Cambridge, MA: Harvard University Press, 2008); and Philip Short, *Mao: A Life* (London, UK: John Murray, 2004).
20. Todd S. Sechser and Matthew Fuhrmann, "Crisis Bargaining and Nuclear Blackmail," *International Organization* 67, no. 1 (January 2013): 173–95, [http://journals.cambridge.org/download.php?file=%2F15014\\_01102A6160BD5A59D208F20AC173CC4B\\_journals\\_\\_INO\\_INO67\\_01\\_S0020818312000392a.pdf&cover=Y&code=ecc42c67acaf6acff41ae708a1ef5e1](http://journals.cambridge.org/download.php?file=%2F15014_01102A6160BD5A59D208F20AC173CC4B_journals__INO_INO67_01_S0020818312000392a.pdf&cover=Y&code=ecc42c67acaf6acff41ae708a1ef5e1). For another argument that states with more nuclear weapons tend to "win" their crises, see Matthew Kroenig, "Nuclear Superiority and the Balance of Resolve: Explaining Nuclear Crisis Outcomes," *International Organization* 67, no. 1 (January 2013): 141–71.
21. In his extensive study, Robert Jervis found that "the amount one learns from another's experience is slight even when the incentives for learning are high and the two actors have

much in common and face the same situation." Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), 241–42.

22. Michael Horowitz, "Spread of Nuclear Weapons"; and Erik Gartzke and Dong Joon Jo, "Bargaining, Nuclear Proliferation and Interstate Disputes," *Journal of Conflict Resolution* 53, no. 2 (April 2009): 209–33.

23. Uhl and Ivkin, "Operation Atom," 299–305.

24. Diane Kunz, *The Economic Diplomacy of the Suez Crisis* (Chapel Hill: University of North Carolina Press, 1991), 116–52; and Fursenko and Naftali, *Khrushchev's Cold War*, 136.

25. Sergei Khrushchev, *Nikita Khrushchev and the Creation of a Superpower*, trans. Shirley Benson (University Park, PA: Pennsylvania State University Press, 2000), 211–12; 264.

26. See Nikita Khrushchev, *Memoirs of Nikita Khrushchev*, vol. 3: *Statesman, 1953–1964*, ed. Sergei Khrushchev, trans. George Shriver (University Park: Pennsylvania State University Press, 2004); Sergei Khrushchev, *Nikita Khrushchev and the Creation*; Sergei Khrushchev, *Khrushchev on Khrushchev: An Inside Account of the Man and His Era* (New York: Little, Brown, and Company, 1990); and William Taubman, *Khrushchev* (New York: Norton, 2003).

27. Miller Center, University of Virginia, "Kremlin Decision Making Project (KDMP), October 22, 1962," n.d., <http://millercenter.org/scripps/archive/kremlin>. See also Fursenko and Naftali, *Khrushchev's Cold War*, 465–92.

28. Michael Dobbs, *One Minute to Midnight: Kennedy, Khrushchev and Castro on the Brink of Nuclear War* (New York: Knopf, 2008), 112; and Fursenko and Naftali, *One Hell of a Gamble*, 352.

29. "Minutes of Conversation between the Delegations of the CPCz and the CPSU, The Kremlin (excerpt)," 30 October 1962, History and Public Policy Program Digital Archive, National Archive, Archive of the CC CPCz, (Prague); File: "Antonín Novotný, Kuba," Box 193, <http://digitalarchive.wilsoncenter.org/document/115219>.

30. Norman Cousins, *The Improbable Triumvirate: John F. Kennedy, Pope John, Nikita Khrushchev* (New York: Norton, 1972), 46.

31. Fravel, *Strong Borders, Secure Nation*, 208–09.

32. Lewis and Litai, *Imagined Enemies*, 48.

33. Ibid., 50 footnote (fn) 36, 40.

34. Ibid., 56 fn 79.

35. Ibid., 54 fn 70.

36. Ibid., 57 fn 88; and Macfarquhar and Schoenhals, *Mao's Last Revolution*, 313–14.

37. Lewis and Litai, *Imagined Enemies*, 60.

38. Ibid., 69 fn 146.

39. Fravel, *Strong Borders, Secure Nation*, 216.

40. Rama Lakshmi and Rajiv Chandrasekaran, "Indian Leader Steps Up War Rhetoric," *Washington Post*, 23 May 2002, A16; and David Williams, "Pakistan 'Will Take War to India,'" *Daily Mail* (London), 30 May 2002.

41. Pervez Musharraf, interview by the author, Seattle, WA, March 2010.

42. Pervez Musharraf, presidential address, 27 May 2002, [http://www.satp.org/satporgtp/countries/pakistan/document/papers/Pervez\\_May272002.htm](http://www.satp.org/satporgtp/countries/pakistan/document/papers/Pervez_May272002.htm).

43. Tom Mintier, "Transcript of CNN Interview with Musharraf," transcript, 1 June 2002, <http://asia.cnn.com/2002/WORLD/asiapcf/south/06/01/musharraf.transcript/>.

44. "Transcript of Interview with Pervez Musharraf," *Christian Science Monitor*, 10 September 2002, <http://www.csmonitor.com/2002/0910/p25s02-wosc.html>.

45. "Two Hundred Percent, There Won't Be War": Excerpts from the Pakistan President's Interview with *Washington Post* Editors and Reporters," *OutlookIndia*, 25 June 2003, <http://>

www.outlookindia.com/article.aspx?220543. For a similar claim with explicit reference to the “dangerous confrontation of 2002,” see Musharraf’s speech at the United Nations General Assembly’s 59th Session, 22 September 2004, <http://www.un.org/webcast/ga/59/statements/pakeng040922.pdf>.

46. P. R. Chari, Pervaiz Iqbal Cheema, and Stephen P. Cohen, *Four Crises and a Peace Process: American Engagement in South Asia* (Washington, DC: Brookings Institute Press, 2007), 180, 224. Their index used the *Hindu*, *Times of India*, *Nation*, *Dawn*, *New York Times* and *Washington Post* newspapers.

47. *Ibid.*, 146.

48. Institute for Conflict Management, *South Asian Terrorism Portal*.

49. S. Paul Kapur, “Ten Years of Instability in Nuclear South Asia,” 71–94, 85–86.

50. Keir A. Leiber and Daryl G. Press, “Why States Won’t Give Nuclear Weapons to Terrorists,” *International Security* 38, no. 1 (Summer 2013): 80–104.

51. See Scott D. Sagan, “Why Do States Build Nuclear Weapons? Three Models in Search of the Bomb,” *International Security* 21, no. 3 (Winter 1996–97): 54–86; T. V. Paul, *Power versus Prudence: Why Nations Forgo Nuclear Weapons* (Montreal: McGill-Queen’s University Press, 2000); Etel Solingen, *Nuclear Logics: Contrasting Paths in East Asia and the Middle East* (Princeton, NJ: Princeton University Press, 2007); Jacques Hymans, *The Psychology of Nuclear Proliferation: Identity, Emotions, and Foreign Policy* (Cambridge, UK: Cambridge University Press, 2006); and Jacques Hymans, *Achieving Nuclear Ambitions: Scientists, Politicians, and Proliferation* (New York: Cambridge University Press, 2012).

52. See Mohammad Javad Zarif, “What Iran Really Wants: Iranian Foreign Policy in the Rouhani Era,” *Foreign Affairs* (May/June 2014): <http://www.foreignaffairs.com/articles/141209/mohammad-javad-zarif/what-iran-really-wants>.

53. Joshua R. Itzkowitz Shriffrinson, “A Crude Threat: The Limits of an Iranian Missile Campaign against Saudi Arabian Oil,” *International Security* 36, no. 1 (2011): 167–201.

54. Francis J. Gavin, “Blasts from the Past: Proliferation Lessons from the 1960s,” *International Security* 29, no. 3 (Winter 2004–2005): 100–35.

55. See Simon Henderson, “Policy Alert: Saudi Arabia’s Missile Messaging,” *Washington Institute for Near East Policy*, 29 April 2014, <http://www.washingtoninstitute.org/policy-analysis/view/saudi-arabias-missile-messaging>.

56. Nicholas Miller, “The Secret Success of Nonproliferation Sanctions,” *International Organization* 68, no. 4 (Fall 2014): 913–44.

57. See Harald Muller and Andreas Schmidt, “The Little-known Story of Deproliferation: Why States Give Up Nuclear Weapons Activities,” in *Forecasting Nuclear Proliferation in the 21st Century: The Role of Theory*, ed. William C. Potter and Gaukhar Mukharzhanova (Stanford, CA: Stanford University Press, 2010), 124–58; and Victor Utgoff *The Coming Crisis: Nuclear Proliferation, U.S. Interests and World Order* (Cambridge, MA: MIT Press, 2000).

58. See Matthew Kroenig, “Time to Attack Iran: Why a Strike Is the Least Bad Option,” *Foreign Affairs* 91, no. 1 (January/February 2012): 76–86, <http://www.foreignaffairs.com/articles/136917/matthew-kroenig/time-to-attack-iran>.



## Book Reviews

*Airpower in Afghanistan 2005–10: The Air Commander's Perspectives*, edited by Dag Henriksen. Air University Press, 2014, 335 pp., download at <http://aupress.maxwell.af.mil/books.asp>.

*Airpower in Afghanistan* is not a collection of “there I was at 30,000 feet” war stories; nor is it *Three Cups of Tea*, delving into the culture that makes Afghanistan a unique and challenging place to conduct business. The real strength of the book is revealed in its subtitle, *The Air Commander's Perspectives*. The contributors to this work are the two- and three-star generals who directed the airpower component for both the United States Central Command (USCENTCOM) combined air operations center (CAOC) in Al Udeid, Qatar, and the North Atlantic Treaty Organization's (NATO) International Security Assistance Force (ISAF) headquarters in Kabul.

As compiler and editor Dag Henriksen explains in his introduction, he did not set out to discover the “whys and hows” behind the war in Afghanistan but rather to “bring forward the larger lessons, challenges, and dynamics related to the use of airpower” in that war and “the broader challenges of alliance/coalition warfare” (p. xxiii–xxiv). He correctly observes that Airmen are typically much better at doing what they do at the tactical level than they are at understanding why they do it from a strategic perspective. Given the complex and sometimes divergent nature of such a compilation as this, it is essential the reader not skip over Henriksen's detailed introduction in which he explains his choice of time frame, his inclusion of certain chapters, and the overall nature and employment of airpower in the land-centric struggle in Afghanistan.

Henriksen, a lieutenant colonel in the Royal Norwegian Air Force (RNoAF) and lecturer and head of the airpower and technology department at its academy in Trondheim, holds a PhD in military studies from the University of Glasgow (UK) and is a graduate of the RNoAF Academy and the Norwegian Defence Command and Staff College in Oslo. He served on coalition air staffs during NATO operations in both the Balkans and Afghanistan. Henriksen compiled this book as an exchange officer at the US Air Force Research Institute, Maxwell AFB, Alabama.

Much of the “conflict” in Afghanistan centered on the differing objectives and procedures of NATO/ISAF and USCENTCOM. The former involved more than 40 different nations that contributed varying assets—usually with many strings attached—and often isolated themselves in provincial reconstruction teams (PRT), where they performed independently, absent any concern for the long-term strategic mission of ISAF. When coalition members are so independent and free to withdraw, command and control and mission planning become challenges. Meanwhile, USCENTCOM was a ground-centric command attempting to control an instrument of power it did not fully understand—airpower.

If nine general officers from four NATO nations on both sides of the Atlantic can agree on anything, it would be that airpower in the ground-centric war in Afghanistan was an afterthought in planning yet was expected to be available without fail when needed—the proverbial “911 call.” As Lt Gen Frederik “Freek” Meulman observed, “Discussing airpower as a unilateral military tool gives little meaning. It is paramount

that the use of airpower—like every military tool—be viewed in relation to all other means of power” (p. 70). He tells of a US two-star Airman dispatched to ISAF HQ who was quite literally not given “a seat at the table” but was instead required to stand during morning briefings.

The most dramatic example of disconnect in air-land coordination occurred in the infamous friendly fire incident during Operation Medusa in 2006. For that reason, Henriksen devotes an entire chapter to the episode, written by Canadian Forces retired major general Charles S. “Duff” Sullivan, copresident of the investigation board convened by USCENTAF. Several of the contributors lament the failure to apply lessons learned from Operation Anaconda (2002) to Operation Medusa.

Many of the tensions between NATO/ISAF and USCENTCOM came from their different primary objectives. The former organization focused, as its name implies, on preparing the Afghan National Police and Afghan National Army to assume security responsibilities for their country; whereas, the latter was engaged in a counterterrorism/counterinsurgency (COIN) undertaking, Operation Enduring Freedom. Absent a clear, overarching strategy, ISAF kept reinventing itself. The difference in missions meant it saw itself as a “strategic-level *function*. . . . It did not see itself as an operational war-fighting *command*,” according to Lt Gen William L. Holland, USAF, retired (p. 59). These numerous ISAF reorganizations with their requisite accompaniment of alphabet soup could have been far easier to follow given an occasional organization chart—one of the few shortcomings of the book. General Meulman also notes the lack of a comprehensive ISAF strategy: “It is easy to state that one wants security, stability, development, and good governance, but that is not a strategy” (p. 75).

Running concurrently with the “Internal Strife and Friction,” which defined ISAF, was the lack of coordination between air and ground forces. Maj Gen Jaap Willemse, Royal Netherlands Air Force, retired, noted in the opening chapter, “we did not have enough good, qualitative, overarching discussions between ground and air officers in terms of how we could use our collective resources to achieve better overall results” (p. 15). He also cites the high turnover rate due to short tours of duty as a contributing factor to poor air-land integration. His counterpart at the CAOC, Lt Gen Allen Peck, USAF, retired, noted the need to learn from our (mis)adventures in Afghanistan. “I would not be surprised if 30 years from now people will say, ‘Oh, we have neglected the lessons from Iraq and Afghanistan.’” One of those lessons is “to posture for future conflicts we will need to put more investment in strategically vital air, naval, and special operations forces (SOF) and let domestic surrogates fight the ground war in their own countries” (pp. 20–21). Both Willemse, as ISAF deputy commander for air in Kabul, and Peck, as deputy combined force air component commander in Al Udeid, make the case for their respective commands to control airpower over Afghanistan—an issue that remains unresolved.

Recognizing and accepting the shift to a COIN mission posed challenges to both USCENTCOM and ISAF. Indeed, the latter proved far more conversant in the intricacies of the art. The non-US generals focused on COIN/nation-building in their respective chapters, while the USAF generals dealt primarily with counterterrorism/air operations. For example, contrast retired Royal Netherlands Air Force lieutenant general Jouke Eikelboom’s chapter, “Moving toward Counterinsurgency” (pp. 123–34),

with that of Maj Gen Douglas Raaberg, USAF, retired, “The Shift from Iraq to Afghanistan” (pp. 136–56).

In terms of developing a coherent and effective COIN strategy, the contributors were almost unanimous that Gen David McKiernan, US Army, was the true architect of the plan rather than his more highly touted successors, US Army generals Stanley McChrystal and David Patraeus. Major General Sullivan clearly considered the replacement of McKiernan by McChrystal an act of political expediency by the administration in Washington, asserting that “tragically, politics trumped military vision and brilliance” (p. 226).

In a comprehensive and analytic epilogue, Henriksen summarizes the factors identified by the various air commanders as contributing to the dearth of operational cohesion. His list includes

lack of a unified strategy, unilateral national emphasis on the PRT construct, the division of Afghanistan into regional commands with significant autonomy and lead nations in charge, a loosely defined concept (counterinsurgency) that had no universal acceptance, significant limitations in competence within ISAF HQ involving all the new concepts governing the approach to this war (e.g., counterinsurgency, effects-based approach to operations, and comprehensive approach), lack of resources, and lack of public/political attention during years of televised havoc in Iraq (p. 268).

Despite all the hand-wringing from Airmen over being pushed out of the planning process, Henriksen remarks that “I have yet to hear a strong and influential voice within the airpower community explaining how airpower could have been better utilized to assist the counterinsurgency effort” (p. 278). Clearly, work remains to be done.

While the US military has long been lambasted, and rightfully so, for always “fighting the last war,” it is evident the United States will be facing more counterterrorism and COIN operations such as Afghanistan for decades to come. Therefore, it is essential that anyone involved in designing and/or implementing US national security strategy learn and understand the lessons outlined in this unique and important book. What better way to attain the essence of these lessons learned than through the eyes of the general officers who ran the air segment of the war and are, predominantly, now retired and free to tell it like it was?

**CAPT Jerry L. Gantt, USNR, Retired**

*Former Content Editor, Strategic Studies Quarterly  
Doctoral Candidate in Public Policy, Auburn University*

***Cybersecurity and Cyberwar: What Everyone Needs to Know*, P. W. Singer and Allan Friedman. Oxford University Press, 2014, 306 pp., \$16.95.**

For commercial and government entities alike, cybersecurity has risen to a prominent position over the last several years. WikiLeaks, Stuxnet, Edward Snowden, Shamoon, and a host of other events and personalities punctuate a narrative that has grown almost impossible to ignore. The resignation of retailer Target’s chief executive officer in the wake of a late-2013 data breach demonstrates as well that cybersecurity is far more than a niche technical issue or a national security problem. It is for this reason

that Singer and Friedman's book should attract a wide audience. Riffing on the title, almost everyone does need to know something about this topic.

For years, colleagues have asked me for a general textbook on cyber warfare or conflict. Containing all of the ideas to understand the issues in a single text is a daunting task. Thinkers on cyber issues must grasp concepts from a variety of places. On one side, there are computing and information technology (IT), which are hard to explain to anyone who has not programmed or had other forms of hands on experience. On the other side, there are connection international security and politics, not to mention all sorts of organizational and process issues as well. For these reasons, cybersecurity is something both technical and political. Linking those areas is what represents the initial point from which thinking and scholarship on cybersecurity can advance.

Adhering to the format of Oxford University Press's *What Everyone Needs to Know* series, Singer and Friedman choose to educate in part 1, explain relevance in part 2, and share prescriptions in part 3. This is an arc that makes sense, although they might have gone into even further detail on the functional details of computing and networking in part 1, but there is no significant omission on the topic.

The authors' first section reads more like a brief history of the Internet, and they happily admit, "In just a few pages, we've summed up what it took decades of computer science to create" (p. 25). Some of cyberspace's creation story bleeds into other sections of the book. For instance, former Grateful Dead lyricist and Electronic Frontier Foundation cofounder John Perry Barlow's "Declaration of the Independence of Cyberspace," winds up in the prescriptive section of the book, but the necessary points are present and strung together well enough. Singer and Friedman also understand another point, the concept of cyberspace, something now considered a domain of conflict for the Department of Defense, emerged from a work of science fiction published little more than 30 years ago.

Trickier terrain is the "Why It Matters" section of the book. Descriptions of cyber-attack and the attribution problem begin the section in fairly clinical language, but then the authors make the necessary case for why cybersecurity issues are important. Stuxnet, the first cyberattack known to have produced a significant kinetic effect, directed against the Iranian nuclear enrichment program, receives ample attention. Somewhat disappointing, however, is that Singer and Friedman miss another immensely important geopolitical cyber event: the 2012 Shamoon attack on Saudi Aramco. This omission is more than offset by an important inclusion: the mention of a cyber industrial complex that feeds upon hyperbole (e.g., Electronic Pearl Harbor). What Myriam Dunn Cavelty labeled cyber threat politics in 2007 has become a very real part of the US and international political landscapes. It is good then that Canadian professor Ronald Deibert's reminder of US Pres. Dwight D. Eisenhower's farewell address is presented here to temper fears of cyber Armageddon.

Concluding the book is its third major section, which asks what can be done. The authors make the convincing point that reengineering the Internet is not going to be a cure-all any time soon. While not explicitly stated, the authors recognize that solutions to cybersecurity issues do not generally fall in the areas of technology or policy alone but rather within some mixing of the two. Their inventory of major areas for possible mitigation of cybersecurity issues hits upon all of the significant topics, from Internet governance to information sharing initiatives. Additionally, they provide the correct



summarizing point to close the section, stating that participants in the cyberspace digital ecosystem have responsibilities as well as rights. How those responsibilities scale across governments, commercial entities, and individuals is one of the truly difficult questions for the topic.

In introducing the text, Friedman and Singer assert, “no issue has emerged so rapidly in importance as cybersecurity” (p. 4). With this I agree. Cybersecurity issues have grown to become very important, very quickly. One of the contributing factors to the 2003 Northeast blackout was a software bug in energy management system at an Ohio utility. It should stand as a reminder that so much of the infrastructure upon which our society depends for economic life and social order is dependent upon networked computing technology. The trend of increasing reliance on computing technology should be a major concern, as should the idea that computing can solve many and any problem—a concept social theorist and critic Evgeny Morozov has labeled “solutionism.”

With an IT solution potentially available for any problem, this should be ample inducement for any executive to give *Cybersecurity and Cyberwar* a read. There is often a gross disconnect in most organizations with which I meet on cybersecurity. Generally, the responses I hear on cybersecurity issues are in the vein of, “we have it in hand,” or “the problem is well-managed.” Ultimately, Singer and Friedman provide the opportunity to educate those interested in listening, and it is high time organizational leaders take note of cybersecurity issues. Senior management has had no problem figuring out how to wring productivity and profits through implementation of IT; now it is up to that same management to be acquainted with the attendant downside of that activity. More than any other reason, leaders should read this book to better understand the cybersecurity problem.

**Chris Bronk**

*Assistant Professor*

*Department of Information and Logistics Technology*

*University of Houston*

***Imperial Crossroads: The Great Powers and the Persian Gulf***, edited by Jeffrey R. Macris and Saul Kelly. Naval Institute Press, 2012, 235 pp., \$34.95.

This book provides an excellent survey of Great Power influence in the region, from the Portuguese in the 1600s to the role of the United States in modern times. In addition, the work explores the historical and contemporary roles of India and China in the region. The book provides a useful guide to studying the importance of the region and the interaction between great and regional powers.

The influence of the Portuguese and the Dutch is an often-neglected component of the Great Power history of the Persian Gulf. The analysis of how the Portuguese ultimately failed to establish control in the region was especially interesting. The analysis of the Dutch role in the region ties into the role of economics, specifically the importance of the Dutch East India Company. These case studies provide important analyses of mercantilist economic principles and the significance of international politics.

A large portion of the work deals with Britain's role. An understanding of this role is essential in understanding the development of the British Empire—in particular its attempts to secure the subcontinent from potential Russian encroachment. The work discusses in detail how the British strategy evolved into what would be labeled in the later twentieth century as the Northern Tier strategy, which aimed to keep the Russians away from the Persian Gulf and to safeguard British interests in India. It also discusses the internal problems Britain faced in maintaining its military presence as well as other political and military commitments Britain had to deal with at the end of World War II. This portion of the work illustrates the difficulty of maintaining empire and the eventual economic problems doing so can cause.

A major contribution of this work is that while the British did loosen their military commitments in the region post 1971, they did not disengage completely. This was illustrated by Britain's relations with the sultanate of Oman and its support for Sultan Qaboos bin Said al Said in the aftermath of the coup that brought him to power. The support the British gave to Oman in putting down the rebellion in the Dhofar province is also discussed.

Another major contribution of this work is a discussion of the internal policy formulation in the United States. This includes the development of the Twin Pillar policy, wherein the United States armed Iran and Saudi Arabia. This served several purposes for the United States, as it enabled a strong pro-Western power in the region without directly tying down large numbers of American military forces. In addition, it also enabled the United States to subsidize its defense industry. While this seems to have been a complementary relationship, it also led to some disagreements among allies. The United States wanted to keep a small naval force in the region, which Iran opposed. This illustrates the problems that often occur among great and small power allies. The work also indicates the political discussions within the administration that ultimately led to the establishment of the Carter doctrine.

The book also examines the significance of the Iranian Revolution on American policy in the region, which resulted in the growth of importance of Saudi Arabia in terms of American policy. The work analyzes the internal workings of American foreign policy and the conflict among special interest groups in the US government over arms sales to Saudi Arabia.

Additionally, a major value of this work that is not discussed enough in the literature is the beneficial discussion of the significance of India and China in the Persian Gulf. In the case of India, the work explores possible strategic scenarios. The authors also discuss the historical presence of China in the Persian Gulf, focusing on why the region has become important in Chinese foreign policy. The work also discusses how Chinese policy can be complementary to American strategic objectives.

In conclusion, this work is of immense value on a number of levels. First, it provides a strong historical analysis of Great Power interest in the Persian Gulf that would be valuable to historians as well as international relations scholars specializing in the region. In addition, this work is of considerable worth to historians of the British Empire who would like to get a brief but comprehensive discussion of the development and evolution of British policy in the Middle East. The authors combine in-depth historical analyses with discussion of the evolving military strategies of the Great Powers. Additionally, they analyze the internal domestics of Britain and the United States,

focusing on how these nations' policies evolved over time. The book would also be valuable to scholars of American foreign policy, as it illustrates the development of US policy in the Persian Gulf and highlights the implications domestic politics have on foreign policy.

John Miglietta

Professor of Political Science  
Tennessee State University

***Forging China's Military Might: A New Framework for Assessing Innovation***, edited by Tai Ming Cheung. Johns Hopkins University Press, 2014, 295 pp., \$22.46.

In *Forging China's Military Might*, the authors aspire to provide "an analytical framework to evaluate the nature, dimensions, and spectrum of Chinese innovation" by exploring the degree to which Chinese science and technology and the nation's industrial base are transforming from imitators into innovators (p. 16). The edited volume is a compilation of selected presentations from a 2011 conference on the Chinese defense economy. According to the book's editor, a key difference between this work and the many that have preceded it is that this one addresses a "critical weakness in the examination of Chinese defense issues," attempting to apply a variety of frameworks to the analysis versus the numerous "descriptive, non-theoretical, narrowly focused on China, and without much comparative perspective" works out there (p. 2). To that end, the book is a mix of theoretical approaches and case studies. Despite contributions by several recognized scholars in the field, the functionality of the chapters varies considerably in terms of the book's overall objective. Often, the framework falls flat, struggling to illuminate anything beyond that derived by reliance on more traditional, descriptive methods, sprinkled with insights and informed speculation. While the individual efforts are, generally speaking, useful—especially for those less familiar with the evolving context—they are not eye-opening to those well-versed on the subject.

While the goal of greater theoretical and analytical rigor is admirable, the "models" employed within offer, at best, a very modest advancement over the descriptive, non-theoretical approaches the editor seems to scorn in his introduction. As such, it incrementally adds to the body of work on the subject.

A standout chapter—aside from a very useful introduction—is chapter 1, co-authored by Tai Ming Cheung (the editor), Thomas Mahnken, and Andrew Ross. Here, the authors, taking a broad approach to the subject of innovation—defining its facets, explaining the whys and hows of military innovation, and evaluating the outputs—imitation, adaptation, and genuine innovation (incremental, architectural, modular, and disruptive/radical), aim to deliver a balanced picture of both the scope and pace of Chinese developments. One of the book's chief purposes is to help policy makers avoid two dangers: overestimating and underestimating Chinese military modernization. Overestimation could increase the pressure felt by other states to engage in a competitive regional arms race. Conversely, underestimating China's capability to innovate sets the stage for surprise, should a conflict arise. To that purpose—defusing hyperbole and/or misinterpretation in either direction—the monograph is a welcome prescription.

Regrettably, the book lacks the analytic punch it is striving to deliver. Of course, within the disciplines of social science and strategic studies, this is a persistent craving—the relentless appetite for predictive models that promise to inform decisions. Unfortunately, such an appetite often correlates with a less-than-discriminating palate concerning the efficacy of many such models. The case studies and, for that matter, several “theoretical” chapters are actually quite descriptive, and the explanatory models they offer deliver no surprises. Glimpses into specific sectors of the defense economy, the governing structures, and methodical management changes the Chinese are making to foster innovation do make for interesting reading; they may also give one pause considering how far the Chinese have come in a relatively brief timespan. However, the essays are of marginal utility in terms of improved assessment capacity regarding Chinese innovation, which is the stated underlying rationale for the work.

**Lt Col John H. Modinger, PhD, USAF**  
*US Air Force Academy*



---

### **Mission Statement**

*Strategic Studies Quarterly* (SSQ) is the senior United States Air Force-sponsored journal fostering intellectual enrichment for national and international security professionals. SSQ provides a forum for critically examining, informing, and debating national and international security matters. Contributions to SSQ will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

### **Disclaimer**

The views and opinions expressed or implied in the SSQ are those of the authors and should not be construed as carrying the official sanction of the US Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

### **Comments**

We encourage you to e-mail your comments, suggestions, or address change to: **StrategicStudiesQuarterly@us.af.mil**.

### **Article Submission**

The SSQ considers scholarly articles between 5,000 and 15,000 words from US and international authors. Please send your submission in MicroSoft Word format via e-mail to:

**StrategicStudiesQuarterly@us.af.mil**

---

**Strategic Studies Quarterly (SSQ)**  
155 N. Twining Street, Building 693  
Maxwell AFB, AL 36112-6026  
**Tel (334) 953-7311**  
**Fax (334) 953-1451**

View *Strategic Studies Quarterly* online at <http://www.au.af.mil/au/ssq/>

**Free Electronic Subscription**

**A forum for critically examining,  
informing, and debating national and  
international security.**



**"Aim High . . . Fly-Fight-Win"**

